**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | | |
|---|---|---|
| In re Patent of: | Gregory G. Raleigh | |
| U.S. Patent No.: | 8,639,811 | Attorney Docket No.: 39843-0180IP1 |
| Issue Date: | January 28, 2014 | |
| Appl. Serial No.: | 13/742,312 | |
| Filing Date: | January 15, 2013 | |
| Title: | AUTOMATED DEVICE PROVISIONING AND ACTIVATION | |

**Mail Stop Patent Board**
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

# PETITION FOR *INTER PARTES* REVIEW OF UNITED STATES PATENT NO. 8,639,811 PURSUANT TO 35 U.S.C. §§ 311–319, 37 C.F.R. § 42

**TABLE OF CONTENTS**

I. REQUIREMENTS FOR IPR ..... 1
A. Grounds for Standing ..... 1
B. Challenge and Relief Requested ..... 1
C. Claim Construction ..... 3
II. THE '811 PATENT ..... 3
A. Brief Description ..... 3
B. Prosecution History ..... 3
III. THE CHALLENGED CLAIMS ARE UNPATENTABLE ..... 4
A. GROUND 1A: Rao renders claims 1, 3, 6, 8-11, 14, and 19-20 obvious ..... 4
1. Rao ..... 4
2. Analysis ..... 9
B. Ground 1B: Rao-Panpaliya renders claim 2 obvious ..... 28
1. Rao-Panpaliya ..... 28
(a) Panpaliya ..... 28
(b) Combination ..... 29
2. Analysis ..... 30
C. Ground 1C: Rao-Jones renders claims 4, 13, 21, 23, and 25 obvious ..... 31
1. Rao-Jones ..... 31
(a) Jones ..... 31
(b) Combination ..... 32
2. Analysis ..... 38
D. Ground 1D: Rao-Jones-Jajoo renders claim 17 obvious ..... 44
1. Rao-Jones-Jajoo ..... 44
(a) Jajoo ..... 44
(b) Combination ..... 45
2. Analysis ..... 47
E. Ground 1E: Rao-Jones-Cole renders claim 22 obvious ..... 48
1. Rao-Jones-Cole ..... 48
(a) Cole ..... 48
(b) Combination ..... 50
2. Analysis ..... 52
F. Ground 1F: Rao-Montemurro renders claim 5 obvious ..... 53
1. Rao-Montemurro ..... 53
(a) Montemurro ..... 53
(b) Combination ..... 54
2. Analysis ..... 55
G. Ground 1G: Rao-Akhtar renders claim 7 obvious ..... 55
1. Rao-Akhtar ..... 55

(a) Akhtar ..... 55
(b) Combination ..... 56
2. Analysis ..... 57
H. Ground 1H: Rao-Ramesh renders claim 18 obvious ..... 59
1. Rao-Ramesh ..... 59
(a) Ramesh ..... 59
(b) Combination ..... 60
2. Analysis ..... 61
I. Ground 1I: Rao-Freund renders claims 12, 15-16, 26-27, and 29-30 obvious ..... 63
1. Rao-Freund ..... 63
(a) Freund ..... 63
(b) Combination ..... 65
2. Analysis ..... 69
J. Ground 1J: Rao-Freund-Bedi renders claim 28 obvious ..... 72
1. Rao-Freund-Bedi ..... 72
(a) Bedi ..... 72
(b) Combination ..... 73
2. Analysis ..... 73
K. Ground 2: Rao-Pregont-Jones renders claims 1 and 24 obvious ..... 74
1. Rao-Pregont-Jones ..... 74
(a) Pregont ..... 74
(b) Combination ..... 76
2. Analysis ..... 78
IV. §314(a) DISCRETION SHOULD NOT PRECLUDE INSTITUTION ..... 80
V. CONCLUSION AND FEES ..... 81
VI. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1) ..... 81
A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1) ..... 81
B. Related Matters Under 37 C.F.R. § 42.8(b)(2) ..... 82
C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3) ..... 82
D. Service Information ..... 82

**EXHIBITS**

SAMSUNG-1001 U.S. Patent No. 8,639,811 to Raleigh ("the '811 Patent")

SAMSUNG-1002 Excerpts from the Prosecution History of the '811 Patent ("the Prosecution History")

SAMSUNG-1003 Declaration and Curriculum Vitae of Dr. Patrick McDaniel

SAMSUNG-1004 Complaint for Patent Infringement in *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al.*, 2-23-cv-00641 (EDTX), Dec. 29, 2023)

SAMSUNG-1005 U.S. Pat. App. Pub. No. 2006/0039354 ("Rao")

SAMSUNG-1006 U.S. Pat. No. 8,285,850 ("Jones")

SAMSUNG-1007 U.S. Pat. No. 8,400,491 ("Panpaliya")

SAMSUNG-1008 U.S. Pat. App. Pub. No. 2009/0207817 ("Montemurro")

SAMSUNG-1009 U.S. Pat. App. Pub. No. 2009/0185527 ("Akhtar")

SAMSUNG-1010 U.S. Pat. App. Pub. No. 2008/0162981 ("Jajoo")

SAMSUNG-1011 U.S. Pat. App. Pub. No. 2009/0228951 ("Ramesh")

SAMSUNG-1012 U.S. Pat. App. Pub. No 2007/0032230 ("Pregont")

SAMSUNG-1013 U.S. Pat. No. 5,987,611 ("Freund")

SAMSUNG-1014 RESERVED

SAMSUNG-1015 Memorandum, Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation (USPTO June 21, 2022) ("Director's Guidance")

SAMSUNG-1016 Samsung Stipulation Letter

SAMSUNG-1017 Federal Court Management Statistics (December 31, 2023)

SAMSUNG-1018 RESERVED

SAMSUNG-1019 van Beek, et. al., 2004, January. Adaptive streaming of high-quality video over wireless LANs. In Visual Communications and Image Processing 2004 (Vol. 5308, pp. 647-660). SPIE. ("van Beek")

SAMSUNG-1020 IETF RFC 791, Internet Protocol, September 1981, downloaded from the internet at https://www.ietf.org/rfc/rfc791.txt on July 28, 2023

SAMSUNG-1021 IETF RFC 5246, The Transport Layer Security (TLS) Protocol, version 1.2, August 2008, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc5246 on May 9, 2024

SAMSUNG-1022 Internet connection speed recommendations, downloaded from the Internet at https://help.netflix.com/en/node/306 on April 29, 2024. ("Netflix")

SAMSUNG-1023 Apostolopoulos, et al., 2002. Video streaming: Concepts, algorithms, and systems. HP Laboratories, report HPL-2002-260, pp.2641-8770. ("Apostolopoulos")

SAMSUNG-1024 U.S. Pat. App. Pub. No. 2006/0282566 ("Virdi")

SAMSUNG-1025 U.S. Pat. App. Pub. No. 2005/0080904 ("Green")

SAMSUNG-1026 IETF RFC 793, TRANSMISSION CONTROL PROTOCOL, September 1981, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc793 on April 24, 2024. ("TCP")

SAMSUNG-1027 U.S. Pat. App. Pub. No. 20070121615 ("Weill")

SAMSUNG-1028 RESERVED

SAMSUNG-1029 U.S. Pat. App. Pub. No. 2008/0080458 ("Cole")

SAMSUNG-1030 U.S. Pat. App. Pub. No. 2010/0281154 ("Bedi")

SAMSUNG-1031 Lobo, et. al., (1999). A policy description language. AAAI/IAAI, 1999, 291-298. ("Lobo")

SAMSUNG-1032 Verma, et. al., (2002). Policy-based management of content distribution networks. IEEE network, 16(2), 34-39. ("Verma")

SAMSUNG-1033 RESERVED

SAMSUNG-1034 Banchs, et. al., Distributed weighted fair queuing in 802.11 wireless LAN, 2002 IEEE International Conference on Communications, Conference Proceedings. ICC 2002 pp. 3121-3127), 2002 ("Banchs")

SAMSUNG-1035 Wu, et. al., 2001. Scalable video coding and transport over broadband wireless networks. Proceedings of the IEEE, 89(1), pp.6-20.

SAMSUNG-1036 IETF RFC 2205, Resource ReSerVation Protocol (RSVP), version 1 Functional Specification, September 1997, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc2205 on May 16, 2024

SAMSUNG-1037 Excerpts, Computer Networks, Fourth Edition, by Andrew Tanenbaum, Prentice Hall, 2003

SAMSUNG-1038 U.S. Pat. App. Pub. No. 2007/0258459 ("Smith")

SAMSUNG-1039 Agrawal, et. al., 2005. Policy-based management of networked computing systems. IEEE Communications Magazine, 43(10), pp.69-75 ("Agrawal")

SAMSUNG-1040 RESERVED

SAMSUNG-1041 Blake, et al., IETF RFC 2475, "An Architecture for Differentiated Services," December 1998, downloaded from the internet at https://datatracker.ietf.org/doc/html/rfc2475 on July 29, 2023

SAMSUNG-1042 Reeder, et. al., 2007. Usability challenges in security and privacy policy-authoring interfaces. In Human-Computer Interaction–INTERACT 2007: 11th IFIP TC 13 International Conference, Rio de Janeiro, Brazil, September 10-14, 2007, Proceedings, Part II 11 (pp. 141-155). Springer Berlin Heidelberg.

SAMSUNG-1043 Mansour, et al., 2001. Jitter control in QoS networks. IEEE/ACM Transactions On Networking, 9(4), pp.492-502.

SAMSUNG-1044 Westerinen, et al., IETF RFC 3198, Terminology for Policy-Based Management, November 2001, downloaded from the Internet on May 27, 2024.

SAMSUNG-1045 Damianou, et al., 2001. The ponder policy specification language. In Policies for Distributed Systems and Networks: International Workshop, POLICY 2001 Bristol, UK, January 29–31, 2001 Proceedings (pp. 18-38). Springer Berlin Heidelberg. ("Damianou")

SAMSUNG-1046 Stone, G.N., Lundy, B. and Xie, G.G., 2001. Network policy languages: a survey and a new approach. IEEE network, 15(1), pp.10-21. ("Stone")

SAMSUNG-1047 Agrawal, et. al., 2007, May. Issues in designing a policy language for distributed management of IT infrastructures. In 2007 10th IFIP/IEEE International Symposium on Integrated Network Management (pp. 30-39). IEEE. ("Agrawal-2")

SAMSUNG-1048 Simplified Policy Language (CIM-SPL). Document Number DSP0231, version, 1. ("CIM-SPL")

SAMSUNG-1049 Ponnappan, et al., 2002, June. A policy based QoS management system for the IntServ/DiffServ based Internet. In Proceedings Third International Workshop on Policies for Distributed Systems and Networks (pp. 159-168). IEEE. ("Ponnappan")

SAMSUNG-1050 Gonçalves, et al., 2009, October. A graphical user interface for policy composition in CIM-SPL. In 2009 International Conference on Ultra Modern Telecommunications & Workshops (pp. 1-7). IEEE. ("Gonçalves")

SAMSUNG-1051 U.S. Pat. App. Pub. No. 2008/0122796 ("Jobs")

SAMSUNG-1052 Grossman, Invention of the year: The iPhone. Time Magazine Online, 1, downloaded from the internet at https://content.time.com/time/specials/2007/article/0,28804,1677329_1678542_1677891,00.html on May 28, 2024.

SAMSUNG-1053 Excerpts, Telcom Dictionary, Althos Publishing, 2007.

SAMSUNG-1054 U.S. Pat. App. Pub. No. 2008/0002652. ("Gupta")

SAMSUNG-1055 U.S. Pat. No. 8,019,868 ("Rao-2")

**CLAIMS**

| Claim | Identifier | Claim Language |
|---|---|---|
| 1 | [1.1] | A wireless device, comprising: |
| | [1.2] | one or more modems for enabling the wireless device to communicate over at least a first wireless network; |
| | [1.3] | a user interface; |
| | [1.4] | memory configured to store a control policy associated with a first application on the wireless device, the first application at least enabling the wireless device to access at least a first data service over the first wireless network; and |
| | [1.5] | one or more processors configured to execute one or more machine-executable instructions that, when executed by the one or more processors, cause the one or more processors to: |
| | [1.6] | assist in obtaining a user input through the user interface, |
| | [1.7a] | determine at least an aspect of the control policy based on the user input, |
| | [1.7b] | the at least an aspect of the control policy for at least assisting in restricting or preventing a first access to the first wireless network by the first application when the first application is executing, |
| | [1.7c] | the at least an aspect of the control policy enabling a first control of the first access to the first wireless network by the first application when the first application is executing that differs from a second control of a second access to the first wireless network by a second application on the wireless device, and |

| | | |
|---|---|---|
| | [1.8] | apply the control policy, thereby at least assisting in restricting or preventing the first access to the first wireless network by the first application when the first application is executing. |
| 2 | [2] | The wireless device recited in claim 1, wherein the first application is configured to at least assist in restricting or preventing the first access to the first wireless network by the first application when the first application is executing. |
| 3 | [3] | The wireless device recited in claim 1, wherein restricting or preventing the first access to the first wireless network by the first application when the first application is executing comprises restricting communication associated with the first application over the first wireless network when the first application runs as a background process. |
| 4 | [4] | The wireless device recited in claim 1, wherein restricting or preventing the first access to the first wireless network by the first application comprises preventing communication associated with the first application over the first wireless network when the first application runs as a background process. |
| 5 | [5] | The wireless device recited in claim 1, wherein the first wireless network comprises a cellular network, a roaming network, or an access network associated with a cost. |
| 6 | [6] | The wireless device recited in claim 1, wherein apply the control policy comprises at least assist in routing or directing at least a portion of traffic associated with the first application over the first wireless network to a particular network communication end point, route, or tunnel. |

| | | |
|---|---|---|
| 7 | [7] | The wireless device recited in claim 1, wherein apply the control policy comprises identify or insert a flow tag in a traffic flow associated with the first application, the flow tag configured to assist in preserving the association of the traffic flow with the first application when the traffic flow is processed by one or more functions of the wireless device that operate on the traffic flow. |
| 8 | [8] | The wireless device recited in claim 1, wherein apply the control policy comprises use an application programming interface to communicate with a software component that at least assists in restricting or preventing the first access to the first wireless network by the first application when the first application is executing. |
| 9 | [9] | The wireless device recited in claim 1, wherein apply the control policy comprises use an application programming interface to communicate information to a software component that at least assists in restricting or preventing the first access to the first wireless network by the first application when the first application is executing, the information being associated with: (a) the first wireless network, (b) a cost associated with the first wireless network, (c) a connection state of the first wireless network, (d) a user preference, or a combination of these. |
| 10 | [10] | The wireless device recited in claim 1, wherein apply the control policy comprises use an application programming interface to communicate with a software component that at least assists in controlling an e-mail transfer option, a media content resolution, or a compression level. |
| 11 | [11] | The wireless device recited in claim 1, wherein apply the control policy comprises use an application programming interface to communicate with a software component that at least assists in controlling a background access. |

| | | |
|---|---|---|
| 12 | [12] | The wireless device recited in claim 1, wherein the control policy is further based on a relationship between a usage limit and a measure of usage of the first wireless network associated with the first application. |
| 13 | [13] | The wireless device recited in claim 1, wherein the control policy is further based on a network administrator input. |
| 14 | [14] | The wireless device recited in claim 1, wherein the user input comprises a directive to restrict, block, disable, turn off, throttle, delay, quarantine, or shape at least a portion of traffic over the first wireless network associated with the first application. |
| 15 | [15] | The wireless device recited in claim 1, wherein the user input comprises a directive to restrict, block, throttle, delay, quarantine, or shape at least a portion of traffic over the first wireless network associated with the first application when an amount or cost of usage of the first wireless network associated with the first application satisfies a condition relative to a threshold. |
| 16 | [16] | The wireless device recited in claim 15, wherein the user input further comprises an indication of the threshold or information associated with the threshold. |
| 17 | [17] | The wireless device recited in claim 1, wherein the user input comprises a directive to restrict, block, throttle, delay, quarantine, or shape at least a portion of traffic over the first wireless network associated with the first application when a quality of a second wireless network satisfies a condition relative to a threshold. |
| 18 | [18] | The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to: assist in establishing a secure control link between the wireless device and a network element , the secure control link secured by an encryption protocol and configured to support control-plane communications between the wireless device and the network element, and obtain at least a portion of the control policy from the network element over the secure control link. |

| | | |
|---|---|---|
| 19 | [19] | The wireless device recited in claim 1, wherein the control policy at least assists in controlling the second access to the first wireless network by the second application on the wireless device, and wherein the user input is a first user input, and wherein the at least an aspect of the control policy is a first aspect of the control policy, and wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to: assist in obtaining a second user input through the user interface, and determine at least a second aspect of the control policy based on the second user input, the at least a second aspect of the control policy for at least assisting in controlling the second access to the first wireless network by the second application on the wireless device. |
| 20 | [20] | The wireless device recited in claim 1, wherein the control policy assists in controlling a third access to a second wireless network by the first application. |
| 21 | [21] | The wireless device recited in claim 20, wherein the at least an aspect of the control policy is further based on a characteristic of the first wireless network or the second wireless network. |
| 22 | [22] | The wireless device recited in claim 20, wherein the at least an aspect of the control policy is further based on a user preference comprising a directive to allow access to the second wireless network by the first application based on a characteristic of the first wireless network. |
| 23 | [23] | The wireless device recited in claim 1, wherein the control policy is a first control policy, and wherein the memory is further configured to store a second control policy associated with the first application, the second control policy for at least assisting in controlling a third access to a second wireless network by the first application when the first application is executing, and wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to apply the second control policy. |

| | | |
|---|---|---|
| 24 | [24] | The wireless device recited in claim 1, wherein the first application is configured to assist in providing a forwarding service, the forwarding service for forwarding traffic between (a) one or more other devices communicatively coupled to the wireless device over a second network and (b) a network system communicatively coupled to the wireless device over the first wireless network, and wherein the at least an aspect of the control policy at least assists in determining whether the forwarding service is available to one or more of the one of more other devices. |
| 25 | [25] | The wireless device recited in claim 1, wherein the wireless device is capable of being communicatively coupled to an intermediate networking device over the first wireless network, the intermediate networking device providing a forwarding service for forwarding traffic between the wireless device and a network system communicatively coupled to the intermediate networking device over a second wireless network, and wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to determine the at least an aspect of the control policy based on a characteristic of the second wireless network. |
| 26 | [26] | The wireless device recited in claim 1, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to obtain a measure quantifying at least the first access to the first wireless network by the first application. |
| 27 | [27] | The wireless device recited in claim 26, wherein obtain a measure quantifying at least the first access to the first wireless network by the first application comprises determine the measure quantifying at least the first access to the first wireless network by the first application. |

| | | |
|---|---|---|
| 28 | [28] | The wireless device recited in claim 26, wherein obtain a measure quantifying at least the first access to the first wireless network by the first application comprises obtain, from a network element, the measure quantifying at least the first access to the first wireless network by the first application. |
| 29 | [29] | The wireless device recited in claim 26, wherein the measure quantifying at least the first access to the first wireless network by the first application comprises an amount of data, a cost, or a time. |
| 30 | [30] | The wireless device recited in claim 26, wherein, when executed by the one or more processors, the one or more machine-executable instructions further cause the one or more processors to assist in presenting, through the user interface, information based on the measure quantifying at least the first access to the first wireless network by the first application. |

Samsung Electronics Co., Ltd. petitions for *Inter Partes* Review ("IPR") of claims 1-30 ("the Challenged Claims") of U.S. Patent No. 8,639,811 ("the '811 Patent").

## I. REQUIREMENTS FOR IPR

### A. Grounds for Standing

Petitioner certifies that the '811 Patent is available for IPR. Petitioner is not barred or estopped from requesting this review. Petitioner was served with a complaint of infringement of the '811 Patent less than one year ago. SAMSUNG-1004; SAMSUNG-1017.

### B. Challenge and Relief Requested

Samsung requests IPR of the Challenged Claims on the grounds below. Dr. McDaniel provides supporting testimony in his Declaration. SAMSUNG-1003, ¶¶[1]-[404].

| Ground | Claim(s) | §103 |
|---|---|---|
| 1A | **1, 3, 6, 8-11, 14, 19-20** | Rao |
| 1B | **2** | Rao-Panpaliya |
| 1C | **4, 13, 21, 23, 25** | Rao-Jones |
| 1D | **17** | Rao-Jones-Jajoo |
| 1E | **22** | Rao-Jones-Cole |
| 1F | **5** | Rao-Montemurro |
| 1G | **7** | Rao-Akhtar |
| 1H | **18** | Rao-Ramesh |

| Ground | Claim(s) | §103 |
|---|---|---|
| 1I | **12, 15-16, 26-27, 29-30** | Rao-Freund |
| 1J | **28** | Rao-Freund-Bedi |
| 2 | **1, 24** | Rao-Pregont-Jones |

The '811 Patent claims priority as early as 1/28/2009 ("Critical Date"). SAMSUNG-1002, Cover. Petitioner does not concede that the Challenged Claims are entitled to the claimed priority. The references are prior art under §§102(a), 102(b), and/or 102(e).

| Reference | Filing | Publication |
|---|---|---|
| Rao | 7/22/2005 | 6/23/2006 |
| Jones | 1/19/2006 | 10/9/2012 |
| Panpaliya | 8/1/2007 | 3/18/2013 |
| Montemurro | 2/15/2008 | 8/20/2009 |
| Akhtar | 5/24/2007 | 7/23/2009 |
| Jajoo | 12/29/2006 | 7/3/2008 |
| Ramesh | 3/5/2008 | 9/10/2009 |
| Freund | 5/6/1997 | 11/16/1999 |
| Cole | 9/29/2006 | 4/3/2008 |
| Bedi | 12/1/2006 | 11/4/2010 |
| Pregont | 8/8/2005 | 2/8/2007 |

### C. Claim Construction

No formal claim constructions are necessary because "claim terms need only be construed to the extent necessary to resolve the controversy." *Wellman, Inc. v. Eastman Chem. Co.*, 642 F.3d 1355, 1361 (Fed. Cir. 2011. Petitioner reserves the right to respond to any constructions Patent Owner offers or the Board adopts. Petitioner is not conceding that each Challenged Claim satisfies all statutory requirements, nor is Petitioner waiving any arguments concerning claim scope or grounds that can only be raised in district court. For this petition, Petitioner applies prior art in a manner consistent with Patent Owner's allegations of infringement before the district court.

## II. THE '811 PATENT

### A. Brief Description

The '811 Patent is directed to a wireless device that uses policies to control access to wireless networks by applications running on the device. SAMSUNG-1001, Abstract. The device determines aspects of the policy based on user input obtained through a user interface (UI). *Id.*

### B. Prosecution History

Examination of the application that became the '811 Patent included a single prior art rejection, responsive arguments and amendment, and subsequent allowance. SAMSUNG-1002, 690-691, 836-851, 855-863. Notably, the Office never considered any reference forming Grounds 1A-1K or 2. SAMSUNG-1002, 693-735; §IV; SAMSUNG-1003, ¶[91] n.13. These references render the

Challenged Claims obvious, as discussed below.

## III. THE CHALLENGED CLAIMS ARE UNPATENTABLE

### A. GROUND 1A: Rao renders claims 1, 3, 6, 8-11, 14, and 19-20 obvious

#### 1. Rao[1]

Rao discloses a "remote access architecture" for "peer-to-peer communications and remote access connectivity" on a computing device. SAMSUNG-1005, Abstract, [0098]. The system (e.g., Figure 1A, below) includes clients (e.g., computing devices 102) that communicate over a network to other devices, such as servers and server farms. *Id.,* [0086]-[0096]; SAMSUNG-1003, ¶[92].

[1] Descriptions of the references and prior art combinations are incorporated into each mapping. All emphasis is added unless otherwise indicated.

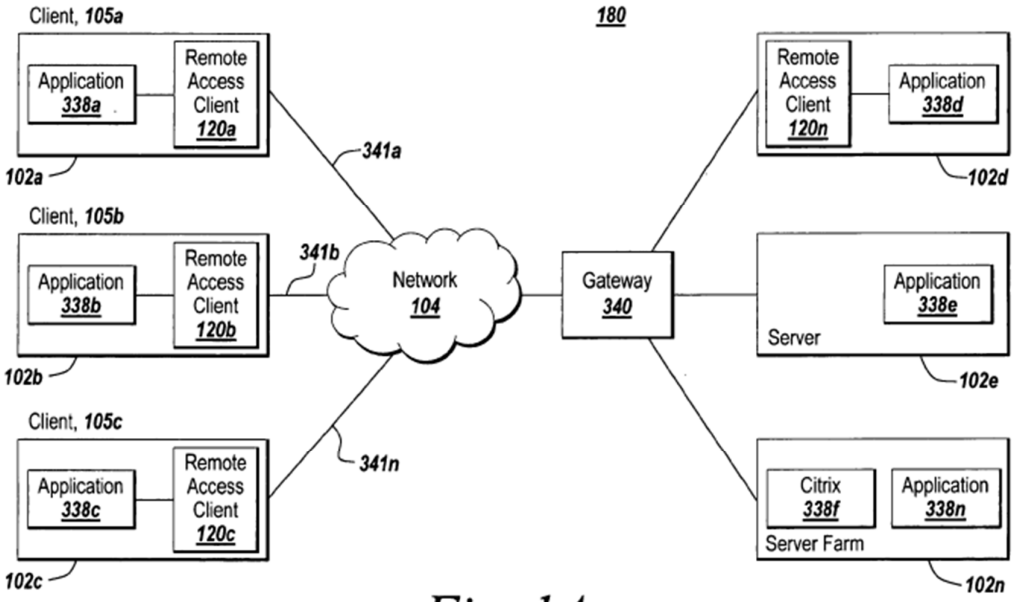



*Fig. 1A*

SAMSUNG-1005, FIG. 1A

Rao addresses inefficient use of network resources when network communications between devices are "processed in the order generated by the activity of a user and applications of the client," which is not "always desirable" because network packets for background applications may be processed ahead of network packets for foreground applications, resulting in applications experiencing increased latency and reduced quality of voice communication. SAMSUNG-1005, [0003]; SAMSUNG-1003, ¶[93].

Rao addresses these inefficiencies through a prioritization scheme that "provide[s] application-aware, client-specific prioritization of packet traffic," which is achieved by augmenting the client with a remote access client (RAC) that interacts with the applications and network stack. SAMSUNG-1005,

[0003], [0089], [0098]-[0100]; SAMSUNG-1003, ¶[94].

Figure 1C shows an example RAC for routing network packets from client to network:

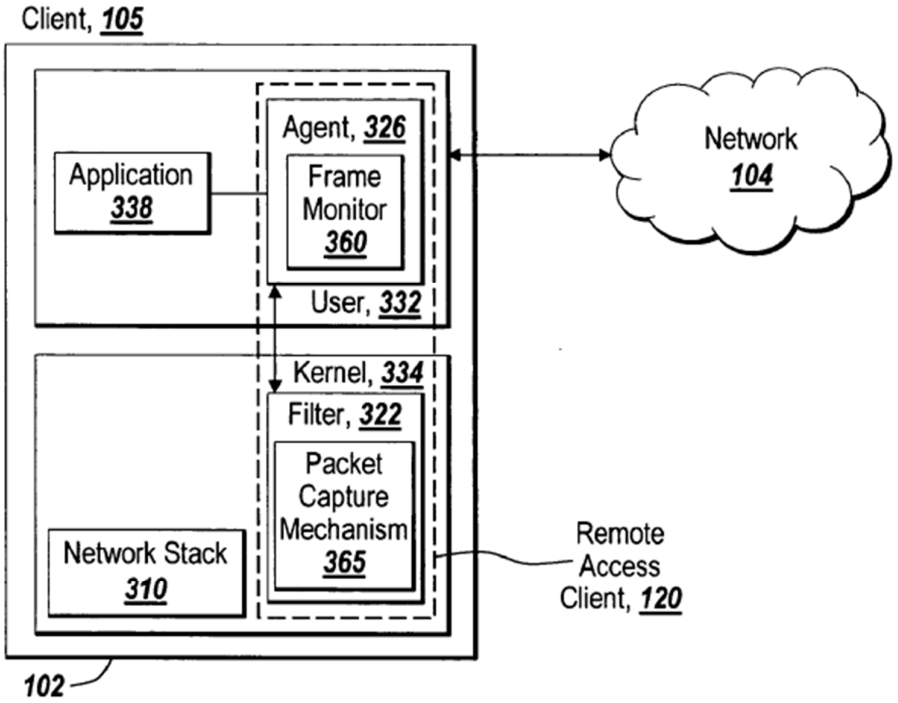



*Fig. 1C*

SAMSUNG-1005, FIG. 1C

RAC can include agent 326 with frame monitor 360 that "include[s] policies and logic for applying a policy to a received packet." *Id.*, [0108]. Frame monitor "transmit[s] a packet to a gateway 340 responsive to a policy-based determination made by the frame monitor." *Id.* The use of policies guides efficient use of network resources and enables Rao's system to address the inefficiencies Rao identifies. SAMSUNG-1003, ¶¶[95]-[96].

Rao's system further enables intelligent and client-centric "prioritization of application network communications on a client based on the type and/or priority of an application." SAMSUNG-1005, [0179], [0182]-[0184], FIG. 5A. To perform prioritization, Rao's system "appl[ies] a policy to determine a condition" of the client, or endpoint, at the time of transmission of the packet." *Id.*, [0109]. Rao's frame monitor can identify an application that generated the packet. *Id.*, [0109]; SAMSUNG-1003, ¶¶[97]-[98].

Figure 5A shows a client providing client-side application-aware network communication:

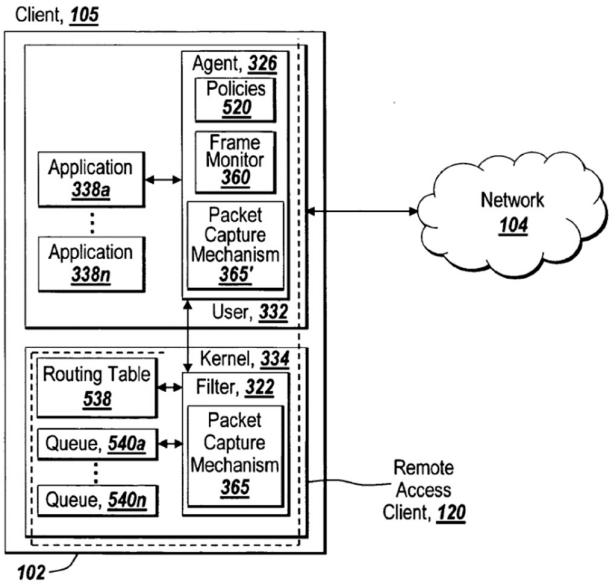



*Fig. 5A*

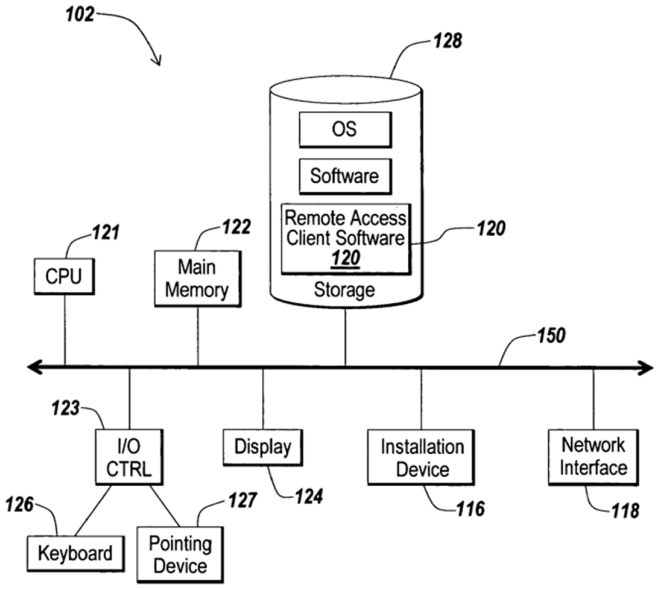
SAMSUNG-1005, FIG. 5A

Rao offers non-limiting disclosure relating to policy specification and

how its system leverages policies for prioritization. SAMSUNG-1005, [0182]-[0184]; SAMSUNG-1003, ¶[100]. Rao describes that policies can be specified, e.g., by name or type of application and type of "protocols used by the applications." SAMSUNG-1005, [0182]. To enable configuration of such policies, Rao's agent "may provide a configuration mechanism such as a user interface, graphical or otherwise, design[ed] and constructed for configuring or specifying the policies." SAMSUNG-1005, [0183].

The Rao Device (RD) includes the various components shown in FIG. 1D (below). SAMSUNG-1005, [0118]. RD's CPU is logic circuitry that responds to and processes instructions fetched from the main memory unit, and is therefore configured to perform or assist in performing the various operations that Rao describes that its device performs. *Id,* [0119]; SAMSUNG-1003, ¶[101], ¶[103].

RD further includes a network interface to interface to networks through a variety of connections including, LAN or WAN links, broadband connections, wireless connections, or some combination. SAMSUNG-1005, [0125]. The network interface can include "a built-in network adapter, network interface card ... wireless network adapter ... modem," etc. *Id.* SAMSUNG-1003, ¶[102].




SAMSUNG-1005, FIG. 1D

## 2. Analysis

### *[1.1]*

To the extent the preamble is limiting, Rao teaches or renders it obvious. SAMSUNG-1003, ¶¶[223]-[225]. Rao teaches a client (RD), as a "wireless end-user device" shown in Figure 1A:

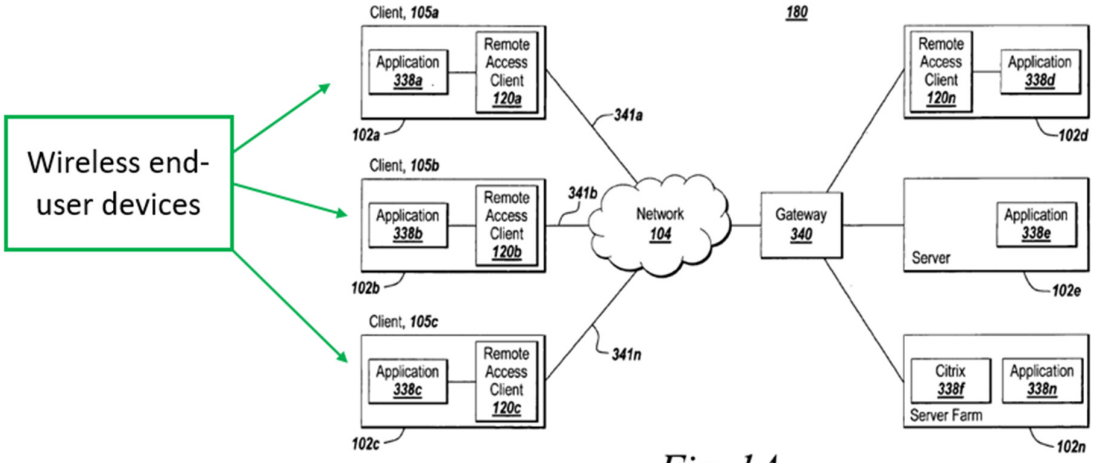



*Fig. 1A*

SAMSUNG-1005, FIG. 1A (annotated), [0086]-[0093]

Rao's environment "includes multiple computing devices" ("clients") connected to a network. SAMSUNG-1005, [0086]. Rao's computing device can be any number of devices, including, "**handheld computer**," "**mobile telephone**," "**smart phone**." SAMSUNG-1003, ¶[225]; SAMSUNG-1005, [0130], [0198].

***[1.2]***

Rao teaches or renders [1.2] obvious. SAMSUNG-1003, ¶¶[226]-[228].

Rao explains that the client "may be ... a smart phone" and describes a wireless modem to communicate data for Internet service activity, e.g., the computing device includes a network interface, which can comprise a "modem." SAMSUNG-1005, [0125], [0172], [0198]; SAMSUNG-1003, ¶[227]. The network interfaces to the Internet through connections, including wireless connections. SAMSUNG-1005, [0095], [0125]; SAMSUNG-1003, ¶[227]. Therefore, Rao teaches that its device includes a network interface (e.g., modem) for communicating over one or more wireless networks. Moreover, a POSITA[2] would have found obvious that Rao's device includes a modem to communicate over a wireless network. SAMSUNG-1003, ¶[228].

***[1.3]***

Rao teaches or renders [1.3] obvious. SAMSUNG-1003, ¶¶[229]-[233].

[2] *See* SAMSUNG-1003, §IV.

Rao's agent provides "a configuration mechanism such as a user interface, graphical or otherwise, design[ed] and constructed for configuring or specifying the policies." SAMSUNG-1005, [0183]; SAMSUNG-1003, ¶¶[230]-[231]. UIs for "configuring or specifying the policies" described in Rao were well-known by the Critical Date and would have been obvious to include for permitting user configurability based on Rao's disclosure and a POSITA's general knowledge of UI technology.[3] SAMSUNG-1003, ¶[230](citing SAMSUNG-1013, SAMSUNG-1048, SAMSUNG-1050). Further, a POSITA would have known or found obvious that the UIs include multiple panels to support device configuration and application needs. SAMSUNG-1003, ¶¶[232]-[233](citing SAMSUNG-1051).

***[1.4]***

Rao teaches or renders [1.4] obvious. SAMSUNG-1003, ¶¶[234]-[241].

Rao's RAC has policies "for specifying client-side prioritization of network communications related to applications," such as email, collaboration, and VoIP. SAMSUNG-1005, 0090], [0179], [0182], [0184]. Because Rao teaches policies "for specifying client-side prioritization of network communications related to applications," and the client can be any type of computing device that runs applications "that access a network" including a "web browser, web-based

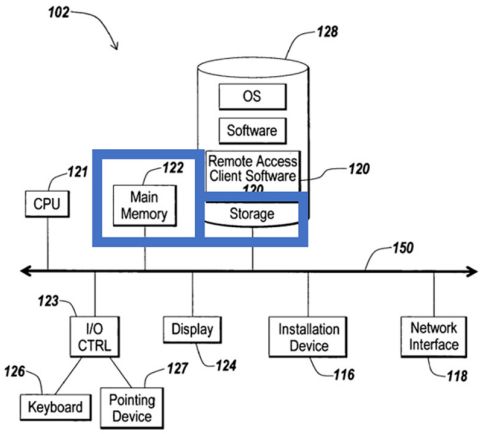
[3] Discussions presented herein reflect a POSITA's knowledge before or at the Critical Date.

client [or] client-server application," a POSITA would have recognized or found obvious that such applications enable the device to access data services, such as server-based services coupled to those applications, over a wired or wireless network. SAMSUNG-1005, [0088], [0090]; SAMSUNG-1003, ¶[235]. For example, Rao explains that its client has applications that communicate to "an application server providing email services such as Microsoft Exchange ... a web or Internet server, or a desktop sharing server, or a collaboration server" and that any of the applications "may comprise any type of hosted service." SAMSUNG-1005, [0090]; SAMSUNG-1003, ¶[236]. Therefore, a POSITA would have recognized or found obvious that Rao's applications enable RD to access data services over Rao's wireless network based on Rao's disclosure of these various data services. SAMSUNG-1003, ¶[237].

Rao's policies are associated with applications. SAMSUNG-1005, [0042], [0182]; SAMSUNG-1003, ¶[238]. For example, Rao's method includes "associating a priority with the first application." SAMSUNG-1005, [0042]; SAMSUNG-1003, ¶[238]. Rao teaches that this association is created via policies that "may be specified by the name of the application," thus associating a particular policy with the named application. SAMSUNG-1005, [0182]; SAMSUNG-1003, ¶[238].

Rao further discloses policies that "may be accessible by the agent" component of Rao's RAC, configured into the agent or loaded by the agent. SAMSUNG-1005, [0183]. A POSITA would have recognized or found obvious that

such policies would be stored in memory on RD, e.g., Rao's "main memory unit" and/or "storage device" which are coupled to Rao's RAC, illustrated in Fig. 1D. SAMSUNG-1005, [0118], Fig. 1D; SAMSUNG-1003, ¶[239].




Rao, FIG. 1D (annotated)

***[1.5]***

Rao teaches or renders [1.5] obvious. SAMSUNG-1003, ¶[242].

RD includes a processor configured to "process[] instructions fetched from the main memory unit." SAMSUNG-1005, [0119], Fig. 1D; §III.A.1.a. The processor executes instructions to perform the operations described in Rao (and in the Rao-based combinations), including the operations mapped to the claim limitations addressed herein. SAMSUNG-1003, ¶[242]; §III.A.1.a.

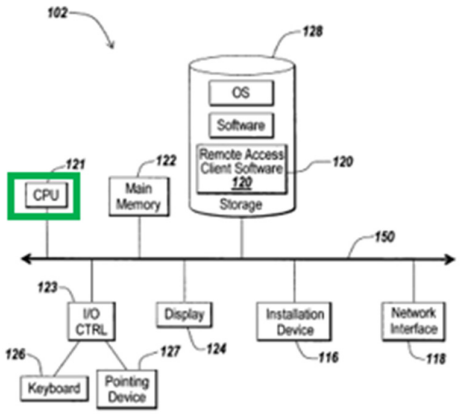



*Fig. 1D*

SAMSUNG-1005, FIG. 1D (annotated)

***[1.6]***

Rao teaches or renders [1.6] obvious. SAMSUNG-1003, ¶¶[243]-[246].

Rao teaches assisting in obtaining user input through a UI, where such input is used to configure policies. SAMSUNG-1003, ¶¶[244]-[245]; III.A.1.c. Rao explains that policies "may be configurable by a user by any suitable means." SAMSUNG-1005, [0183]. For example, the agent "may provide a configuration mechanism such as a user interface, graphical or otherwise, design[ed] and constructed for configuring or specifying the policies." *Id.* A POSITA would have recognized or found obvious that policy UIs that provide input used to create and modify policies were well known by the Critical Date and would have been obvious to include for permitting user configurability based on Rao's disclosure and a POSITA's general knowledge of UI technology. SAMSUNG-1003, ¶[246](citing SAMSUNG-1013, SAMSUNG-1039,

SAMSUNG-0149, SAMSUNG-1050).

***[1.7a]***

Rao teaches or renders [1.7a] obvious. SAMSUNG-1003, ¶[247]-[251].

Rao teaches that "policies" are "configurable by a user by any suitable means," including by using "a user interface" "for configuring or specifying the policies." SAMSUNG-1005, [0183]; SAMSUNG-1003, ¶[248]. In view of Rao's teachings, a POSITA would have recognized or found obvious that policy UIs accept user input used to create and modify policies. *See* [1.6]; SAMSUNG-1003, ¶[249](citing SAMSUNG-1039).

Rao's policies are "specified conditionally" and configured using user input from the UI as discussed above. SAMSUNG-1005, [0182]-[0184]. A POSITA would have understood Rao's policies, therefore, to include a condition aspect comprising one or more clauses of a Boolean expression. SAMSUNG-1003, ¶[250](citing SAMSUNG-1046, SAMSUNG-1047, SAMSUNG-1050). For example, a condition aspect includes clauses that specify the circumstances under which the policy applies, e.g., ***based on the name*** and/or ***based on type of the application***, and can include other Boolean clauses. SAMSUNG-1005, [0182]; SAMSUNG-1003, ¶[250]. Additionally, the condition aspect expressed as the Boolean expression can include fewer clauses, additional clauses or a different set of clauses. SAMSUNG-1003, ¶[250]. An action aspect defines the corresponding action if the Boolean condition is met and includes, e.g., queue priority for packets from the application that determines

queue assignment. SAMSUNG-1005, [0184]; SAMSUNG-1003, ¶[250].

Since Rao's policies are configurable by a UI, a POSITA would have recognized or found obvious that Rao's UI obtains user input that determines the condition aspect of a policy. SAMSUNG-1005, [0182]-[0184]; SAMSUNG-1003, ¶[251]. Determining aspects of policies based on user input from a UI was well known by the Critical Date, and it would have been obvious to use user inputs in determining aspects of Rao's policies based on Rao's disclosure and a POSITA's general knowledge of policy determination and UI technology. SAMSUNG-1003, ¶[251].

***[1.7b]***

Rao teaches or renders [1.7b] obvious. SAMSUNG-1003, ¶¶[252]-[266].

Rao teaches determining, from user input, a condition aspect of a control policy that includes one or more Boolean expressions, e.g., based on the name of the application and/or type of the application. SAMSUNG-1005, [0182]; SAMSUNG-1003, ¶[253]; s*ee* [1.7a].

Rao further teaches that control policies assist in restricting an executing application's access to a wireless network. SAMSUNG-1003, ¶[254]. Rao's policy-based queuing provides "client-side application-aware network communication prioritization." SAMSUNG-1005, [0131]; SAMSUNG-1003, ¶¶[254]-[259]. In Rao, "priorities for applications" are used to "place, arrange, or coordinate network packets into queues" in support of the priorities, and the network

packets are communicated from the queues according to the determined priorities for the network packets. SAMSUNG-1005, [0191], [0194]. Consequently, "real-time data communications of [an] application" are prioritized ahead of other applications. SAMSUNG-1005, [0184].

Rao's teachings apply to a range of applications, including streaming video, email, collaboration, and "any application related to real-time data communications." SAMSUNG-1005, [0088], [0179]; §III.A.1.a; SAMSUNG-1003, ¶[260]. Rao further teaches that application priority is relative, e.g., by "associating a priority with the first application higher than a priority associated with the second application." SAMSUNG-1005, [0042]; SAMSUNG-1003, ¶[260]. Consequently, Rao prevents "network packet[s] of [an] application from being communicated ... ahead of ... network packets of [another] application." SAMSUNG-1005, [0040].

Rao provides an example in which "secure real-time data communications can be communicated from the client at higher priorities than other applications of the client to improve the quality of the real-time experience, such as VoIP." SAMSUNG-1005, [0218]. A POSITA would have recognized that, among Rao's "other applications," it is beneficial to provide real-time, non-interactive applications (e.g., streaming video) priority over non-real-time, non-interactive applications (email), e.g., to avoid video stuttering. SAMSUNG-1003, ¶[261](citing SAMSUNG-1024, SAMSUNG-1025). A POSITA also would have recognized the benefits of prioritizing interactive real-time traffic

(e.g., VoIP) over non-interactive real-time traffic (e.g., streaming video), and prioritizing both over non-real-time traffic. SAMSUNG-1005, [0042], [0218]; SAMSUNG-1003, ¶[261]. Moreover, a POSITA would have recognized or found obvious the use of the name of an application to determine the priority of an application. SAMSUNG-1005, [0182], [0184]; SAMSUNG-1003, ¶[262]. For example, the control policy would specify application priority based on the name of an application, and the priority is based (at least in part) on whether the application provides real-time data communications or is instead non-real-time. SAMSUNG-1003, ¶[262].

Therefore, a POSITA would have known that, in Rao, priority-based queuing is applied such that lower-priority applications are restricted from using the network at least when contention for the network exists, e.g., when multiple applications request transmission. SAMSUNG-1005, [0042], [0179], [0184], [0218]; SAMSUNG-1003, ¶[263]. In such cases, "packets are communicated according to the determined priority." SAMSUNG-1005, [0184]. For example, when video streaming (a non-interactive application) is executing as a first application, Rao's priority-based queuing restricts its network access by placing its packets in a lower-priority queue as compared to packets from higher-priority applications (e.g., an active application such as VoIP). SAMSUNG-1005, [0184], [0218]; SAMSUNG-1003, ¶[263].

Since the condition aspect of a policy determines when to apply the ac-

tion aspect of a policy, a POSITA would have recognized that the condition aspect of a policy (e.g., including a Boolean clause specifying application name) assists in restricting access (of lower priority application) to the network. *See* [1.7a]; SAMSUNG-1003, ¶¶[264]-[265], §VII.B.

Therefore, a POSITA would have recognized or found obvious that at least an aspect of the control policy (condition aspect) assists in restricting access to the first wireless network by the first application (by assigning its packets to a lower-priority queue). SAMSUNG-1005, [0179], [0184]; SAMSUNG-1003, ¶[266].

***[1.7c]***

Rao teaches or renders [1.7c] obvious. SAMSUNG-1003, ¶¶[267]-[274].

Rao teaches or renders obvious that policies include aspects, such as condition aspects and action aspects, which are determined based on user input, and that restrict access to the wireless network, and that differ for different applications (e.g., when conditions are based on application name). SAMSUNG-1003, ¶[268]; *see* [1.7a]-[1.7b]. Thus, Rao teaches or renders obvious that the aspect of the control policy enables a first control of access to the wireless network by the first application that differs from a second control of access to the wireless network by a second application (e.g., by determining a priority for the first application that differs from a priority for the second application, thereby resulting in access to the wireless network being controlled differently for the first and second applications). *Id.*

For example, based on the condition aspect ("at least an aspect"), which includes "***the name of the application***," RAC assigns packet priority, explaining that RAC "determines the association of network packets with applications" to "determine priorities and apply any priority based policies." SAMSUNG-1005, [0182]-[0184], [0187]; SAMSUNG-1003, ¶[269]. Then, "[b]ased on the indicated priorities for applications," the filter may place "network packets into queues" according to priority and "the network packets are communicated from the queues" according to the determined priorities. SAMSUNG-1005, [0191], [0194]; SAMSUNG-1003, ¶[269].

Since Rao teaches a condition aspect (e.g., based at least in part on an application's name) determines the queue for the application's packets, and the queue determines the order of transmission, a POSITA would have recognized or found obvious that the condition aspect enables a first control (e.g., the order of the application's packet transmission). SAMSUNG-1005, [0182]-[0184], [0187], [0191], [0194]; SAMSUNG-1003, ¶[270].

A POSITA would have further recognized or found obvious that, for a second application with a different name, at least in some cases, Rao assigns packets to a different queue. SAMSUNG-1005, [0182]-[0184], [0187], [0191], [0194]; SAMSUNG-1003, ¶[271]. For example, Rao provides an example in which an application "generate[s] real-time data of VoIP communications" and the client, "may prioritize the real-time data communications of [the] application ... ahead of other applications, such as non-real-time data communication

applications." SAMSUNG-1005, [0184]. A POSITA would have known or found obvious that the VoIP application would have a different name than "other applications," and the packets of the two applications are assigned to different queues. SAMSUNG-1003, ¶[272].

Since queues determine the order of transmission, a POSITA would have recognized that the second application name enables, at least in part, a second control (e.g., the order of the second application's packet transmission), which differs from the first control. SAMSUNG-1003, ¶¶[273]-[274].

***[1.8]***

Rao teaches or renders [1.8] obvious. SAMSUNG-1003, ¶¶[275]-[276].

Rao applies control policies that restrict access to the first wireless network by the first application (e.g., non-interactive video streaming) when the first application is executing by assigning its packets to a queue that is not the highest priority. SAMSUNG-1005, [0182]-[0184], [0187], [0191], [0194]; *see* [1.7b], [1.7c]. Specifically, Rao explains that "a priority for the intercepted and queued network packet is determined based on the type and/or priority of the application" and "the network packets are communicated according to the determined priority." SAMSUNG-1005, [0184]; SAMSUNG-1003, ¶[276].

***[3]***

Rao teaches or renders [3] obvious. SAMSUNG-1003, ¶¶[277]-[278].

Rao teaches restricting access to the first wireless network by the first application, and further teaches that the restriction can be "based on whether an

application is running in the foreground or the background of the client." *See* [1.7b]-[1.8]; SAMSUNG-1005, [0182]. A POSITA would have therefore found it obvious to restrict the first access to the first network by assigning packets from the first application (e.g., video streaming) when it is running as a background application to lower-priority queues, thus restricting its communication. SAMSUNG-1005, [0182], [0184]; SAMSUNG-1003, ¶[278]; *see* [1.7b]; *see also* SAMSUNG-1005, [0179]-[0195].

***[6]***

Rao teaches or renders [6] obvious. SAMSUNG-1003, ¶¶[279]-[281].

Rao's RAC uses a routing table that includes "information about a source computing device and a destination computing device to identify a communication path or connection between a source and destination communication points." SAMSUNG-1005, [0181]. A POSITA would have recognized or found obvious that "a communication path" is a route and "destination communication points" are endpoints, and therefore Rao teaches or renders obvious routing or directing traffic to a communication endpoint or route. *Id.*; SAMSUNG-1003, ¶[280].

Additionally, Rao teaches that traffic is assigned to priority queues based on policy. SAMSUNG-1005, [0184]; SAMSUNG-1003, ¶[281]; *see* [1.7b]-[1.7c]. For example, the RAC includes policies for "specifying client-side prioritization of network communications related to applications," and policies can "indicate prioritization based on the destination network address, such as host

name or IP address, and/or destination port number." SAMSUNG-1005, [0182]; SAMSUNG-1003, ¶[281]. A POSITA would have recognized or found obvious that when an application (e.g., video streaming) transmits data to a destination network address, the destination's network address identifies a particular endpoint, and therefore Rao's prioritizing communication based on the endpoint's network address assists in routing and directing traffic from the application and to the endpoint at that network address. SAMSUNG-1005, [0088], [0181]-[0182]; SAMSUNG-1003, ¶[281].

***[8]***

Rao teaches or renders [8] obvious. SAMSUNG-1003, ¶¶[282]-[287].

RD includes an agent and filter that restrict and prevent access to networks by executing applications, including video streaming. SAMSUNG-1003, ¶[282]; *see* [1.7b]-[1.7c], [§III.A.1.a].

In Rao, the client "runs a filter," and the agent "may communicate the priority of network packets to the filter" by any suitable means "such as via an ***application programming interface (API)***." SAMSUNG-1005, [0099], [0190]. The filter arranges packets in the queues "in support of the priorities." SAMSUNG-1005, [0191].

A POSITA would have recognized or found obvious that Rao's filter is a software component that assists in restricting an executing application's access to the network (e.g., access by video streaming) by assigning packets to queues

based on packet priority. *See* [1.7b]; SAMSUNG-1005, [0190]-[0191]; SAMSUNG-1003, ¶[286].

***[9]***

Rao teaches or renders [9] obvious. SAMSUNG-1003, ¶¶[288]-[292].

Rao "communicates the priority of network packets to the filter" using any means, including an API." SAMSUNG-1005, [0190]. Rao's policies, which include packet priorities, are "configurable by a user," thereby reflecting a user preference. SAMSUNG-1005, [0183]; SAMSUNG-1003, ¶[289].

The filter is a software component that assists in restricting access to the network by "plac[ing], arrang[ing], or coordinat[ing] network packets into queues," including packets from the first application (video streaming). SAMSUNG-1005, [0099], [0191]; SAMSUNG-1003, ¶[290]. As discussed in [8], Rao's client "runs a filter," and the agent communicates the priority of network packets to the filter by any means, e.g., "***via an application programming interface (API)***." SAMSUNG-1005, [0099], [0190].

Thus, the information communicated through the API can include information associated with a user preference (e.g., the priority of an application) expressed in a policy that was configured "by a user," and is therefore associated with a user preference. SAMSUNG-1005, [0183]; SAMSUNG-1003, ¶[292].

***[10]***

Rao teaches or renders [10] obvious. SAMSUNG-1003, ¶¶[293]-[295].

Rao teaches an API to communicate with a software component (filter)

that assists in restricting application access. *See [8].*

Rao further teaches that the software component (filter) assists in controlling an email transfer option. SAMSUNG-1003, ¶[295]. For example, Rao teaches that "all network[] packets for a type of application" (e.g., email or VoIP) may be "placed in a queue" used to prioritize network packets for applications, e.g., "online collaboration related applications" can "be placed and prioritized" in a queue for collaboration-related applications and a second queue may be used for email-related applications. SAMSUNG-1005, [0192]. A POSITA would have recognized that placing email packets in a particular priority queue is controlling an e-mail transfer option. SAMSUNG-1003, ¶[295].

***[11]***

Rao teaches or renders [11] obvious. SAMSUNG-1003, ¶¶[296]-[298].

Rao teaches an API to communicate with a software component that assists in restricting application access. *See [8].*

Rao further teaches assisting in controlling background access using the API, explaining that the agent may use characteristics of the application "such as running in the foreground or background, to indicate priority for a network packet of the application." SAMSUNG-1005, [0182]; SAMSUNG-1003, ¶[298].

***[14]***

Rao teaches or renders [14] obvious. SAMSUNG-1003, ¶¶[299]-[302].

As discussed above, in RD, user input determines policies. *See* [1.6]

[1.7a]-[1.7c]; §III.A.1.a; SAMSUNG-1003, ¶[300].

Rao's policies are directives to restrict, throttle and/or delay, at least a portion of the traffic by assigning such traffic to priority-based queues. SAMSUNG-1003, ¶¶[301]-[302]. For example, the filter can place network packets into queues by priority and the packets are communicated from the queues according to the priorities. SAMSUNG-1005, [0191], [0194]. A POSITA would have recognized that priority queues throttle, restrict, and delay traffic based on priority. SAMSUNG-1005, [0184]; SAMSUNG-1003, ¶[302].

***[19]***

Rao teaches or renders [19] obvious. SAMSUNG-1003, ¶¶[303]-[307].

Rao renders obvious the wireless device of claim 1, wherein the control policy assists in controlling the second access to the first wireless network by the second application on the wireless device. *See* [1.7c].

Rao renders obvious user input that is a first user input, and where the at least an aspect of the control policy (condition aspect) is a first aspect of the control policy. *See* [1.6], [1.7a]-[1.7c].

For similar reasons, Rao renders obvious user input that is a second user input, and that the second user input determines a second aspect of the control policy (e.g., condition or action aspect) that controls access to the wireless network for a second application (e.g., assigning different priorities to different applications). *Id.*; SAMSUNG-1003, [306], §VII.B. For example, Rao renders obvious machine-executable instructions that are executed by RD's processors

causing the processor to assist in obtaining a second user input through the UI. SAMSUNG-1003, ¶[306]. Rao's policies include conditions (first aspects, including, e.g., the name of the application, type of application, foreground/background status, etc.), and actions (second aspects), which indicate priority. SAMSUNG-1005, [0182]-[0193]; SAMSUNG-1003, ¶[306]. Further, Rao explains that the agent can provide a configuration mechanism such as a UI designed for specifying the policies. SAMSUNG-1005, [0183]. Therefore, a POSITA would have recognized that policies, including conditions (first aspect of the policy) and actions (second aspect of the policy), are obtained as user input from a UI and determined from that input. *See* [1.6], [1.7a]; SAMSUNG-1003, ¶[306].

Rao renders obvious determining at least a second aspect of the control policy based on the second user input (the action element of the policy) that assists in controlling the second access to the first wireless network by the second application on the wireless device. SAMSUNG-1003, ¶[307]. For example, Rao teaches policies where the action aspect of the policy controls application access to the wireless network by assigning packets to priority queues, including a second access by a second application (e.g., VoIP). SAMSUNG-1005, [0004], [0184]; SAMSUNG-1003, ¶[307].

***[20]***

Rao teaches or renders [20] obvious. SAMSUNG-1003, ¶¶[308]-[310].

RD's policies assist in controlling access to all networks (including a second wireless network) by all applications (including the first application, video streaming). SAMSUNG-1003, ¶[309]; *see* [1.7b], [1.7c]. For example, Rao teaches accessing multiple networks, e.g., the device can include a network interface to interface various networks, e.g., LAN, WAN, Internet, via LAN or WAN links, wireless connections, etc., or using combination of those. SAMSUNG-1005, [0125]. Rao explains that the network interface can include any other device suitable for interfacing the computing device to any type of network capable of communication. *Id.;* SAMSUNG-1003, ¶[309].

A POSITA would have recognized that when RD is connected to a first network (e.g., a home wireless network) the control policy assists in controlling access to the first network, and when RD is connected to a second network (e.g., a work wireless network), the control policies assist in controlling access to the second network. SAMSUNG-1003, ¶[310].

### B. Ground 1B: Rao-Panpaliya renders claim 2 obvious

#### 1. Rao-Panpaliya

##### (a) Panpaliya

Panpaliya teaches adjusting "video parameters of a video communication session based on a type of use for the video communication session," including "applying a profile of video parameters to the session based on the use." SAMSUNG-1007, Abstract. Video parameters include screen size, resolution, buffer size, frames per second, etc. SAMSUNG-1007, 4:64-67.

Video parameters can be adjusted based on a detected network constraint, where a "network constraint detection component" monitors "the current network parameters associated with an existing video communication session ... to detect if a network constraint exists." SAMSUNG-1007, Abstract, 5:66-6:3.

When the network constraint detection component "determines that an unfavorable threshold level has been reached, a network constraint is detected" and the system "adjusts video parameters in a manner that continues to provide an acceptable user experience." SAMSUNG-1007, 6:7-12.

(b) **Combination**

As described above, RD prioritizes packets according to priority. *See* §III.A.1.a; SAMSUNG-1003, ¶[109]. However, a POSITA would have recognized that prioritizing packets does not address insufficient bandwidth to transmit video, and would have looked to references such as Panpaliya, which teaches that multimedia data can be adjusted to meet network constraints (e.g., reducing the quality, and thus amount of data to be transferred, in response to limited bandwidth). SAMSUNG-1007, Abstract, 6:65-67, 5:66-6:3, 6:64-66; SAMSUNG-1003, ¶¶[110]-[115]. Consequently, a POSITA would have recognized that, by applying the techniques of Panpaliya, multimedia data (e.g., Rao's video) can be streamed over a bandwidth-constrained network, albeit at reduced quality. SAMSUNG-1005, [0004]; SAMSUNG-1003, ¶[115].

In operation, the resulting Rao-Panpaliya device (RPD) adjusts video parameters based on detected network constraints (if any exist),[4] then transmits the adjusted video stream using policy-based priority queuing (per Rao). SAMSUNG-1003, ¶[116].

**2. Analysis**

***[2]***

RPD renders [2] obvious. SAMSUNG-1003, ¶¶[311]-[313].

In Panpaliya, a "network constraint detection component" monitors "the current network parameters associated with an existing video communication session ... to detect if a network constraint exists," and when it "determines that an unfavorable threshold level has been reached, a network constraint is detected" and the system "adjusts video parameters in a manner that continues to provide an acceptable user experience." SAMSUNG-1007, 5:66-6:12. SAMSUNG-1003, ¶[312].

When RPD runs a first application (e.g., the video streaming application of Rao, which instantiates a video communication session of Panpaliya), it detects a network constraint (e.g., insufficient bandwidth) and restricts access to the wireless network by "adjusting one or more video parameters of a video communication session," such as the frame rate, which reduces (restricts) the

[4] If sufficient bandwidth exists, RPD need not adjust the video. SAMSUNG-1003, ¶[116] n.16.

bandwidth demand. SAMSUNG-1005, [0088]; SAMSUNG-1007, Abstract, 4:62-67, 5:27-35; SAMSUNG-1003, ¶[313].

### C. Ground 1C: Rao-Jones renders claims 4, 13, 21, 23, and 25 obvious

#### 1. Rao-Jones

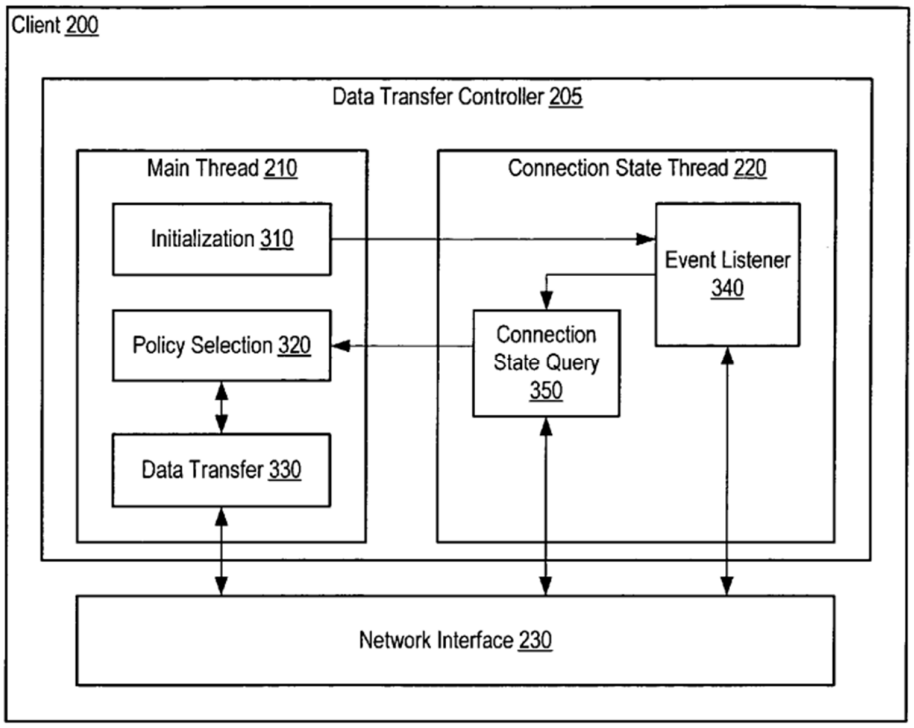
##### (a) Jones

Jones discloses techniques for "managing data transfers between client computers and a computer network" in which client devices include a "data transfer controller" and "data transfer rules." SAMSUNG-1006, Abstract. Jones explains that "it has become common for client computers to be dynamically connected to the enterprise network through a variety of connection types" and that the "method of connection ... may change frequently as the mobile user travels from place to place." *Id.*, 1:11-17. Jones' mobile devices connect to multiple networks, where each mobile computer may connect to a network via modem, wireless LAN, wireless WAN, etc., and the capabilities of each connection, such as connection speed, vary from one type to another. *Id.*, 3:17-29.

Jones further explains that "[b]ecause of the differing capabilities of various connection types, it is generally desirable for software applications to be able to determine if and when a network connection changes" and that "[t]here are a variety of ways to determine the characteristics of a network connection," such as using API calls. SAMSUNG-1006, 1:30-36. For example, "if the connection type is slow, such as via a modem, a user who is attempting to access e-

mail or browse the internet may be frustrated as the available bandwidth is consumed by backup data transfers." *Id.*, 3:55-58. Therefore, it is desirable for policies to "adjust the frequency of data backups according to ... the type of connection, and/or the bandwidth of the connection." *Id.*, 3:60-67.

To provide such policy-based management, Jones teaches a client that fetches the current state of the network interface and forwards it to a policy selection component that applies rule(s) for data transfer. SAMSUNG-1006, 4:27-48, FIG. 3.




SAMSUNG-1006, FIG. 3

(b) **Combination**

Rao provides techniques for optimizing peer-to-peer communications, in-

cluding real-time communications using "application-aware prioritization of client-side network communications," where one application is granted a higher priority than another for access to network resources. SAMSUNG-1005, [0004], [0088], [0184]. Rao's prioritization addresses situations where a client device is running both real-time and non-real-time applications. *Id.*, [0003]; SAMSUNG-1003, ¶[122]. Without Rao's prioritization, packets from the non-real-time application "may be processed ahead of the real-time network packets," increasing their latency. SAMSUNG-1005, [0003]; SAMSUNG-1003, ¶[122]. A POSITA would have recognized that Rao's teachings apply to packets from other real-time applications, such as streaming video. SAMSUNG-1003, ¶[122].

Interactive applications such as streaming media and interactive games have real-time network constraints, such as bandwidth and latency, and Rao implies that delaying non-real-time traffic from these types of applications (by assigning such traffic to low-priority queues) is sufficient to meet the requirements of real-time traffic. SAMSUNG-1003, ¶¶[123]-[124](citing SAMSUNG-1023). A POSITA would have recognized that, when available networks cannot meet such real-time constraints, even queuing will not provide an acceptable user experience. SAMSUNG-1003, ¶[126].

In some cases, the network simply lacks the capacity to support an application (e.g., insufficient bandwidth to stream video). SAMSUNG-1003, ¶[126];

SAMSUNG-1019, 1. In such cases, allowing the application to access the network not only provides a poor user experience for that application (e.g., showing video that stutters and freezes), but also saps network capacity from other applications. SAMSUNG-1003, ¶¶[127](citing SAMSUNG-1019). Therefore, a POSITA would have recognized that denying access to the application is preferred, altogether avoiding contention and preserving bandwidth for applications that can operate properly in the available bandwidth. SAMSUNG-1003, ¶[130].

Jones explains that, in other cases, while the network possesses sufficient capacity to support a particular application, it lacks capacity to simultaneously support *multiple* applications. SAMSUNG-1006, 1:54-58; SAMSUNG-1003, ¶[128]. For example, "if the connection type is slow ... a user who is attempting to access e-mail ... may be frustrated as the available bandwidth is consumed by backup data transfers." SAMSUNG-1006, 1:54-58.

In such cases, while sufficient bandwidth exists to serve a first application (e.g., email, multimedia streaming, etc.), network use by other applications can limit available bandwidth such that the first application cannot provide an acceptable user experience. SAMSUNG-1006, 1:54-58. Therefore, a POSITA would have recognized that a lack of bandwidth can be caused both by a slow network and by network contention (e.g., the network cannot satisfy aggregate bandwidth demands). SAMSUNG-1003, ¶[129]. In both cases, a POSITA

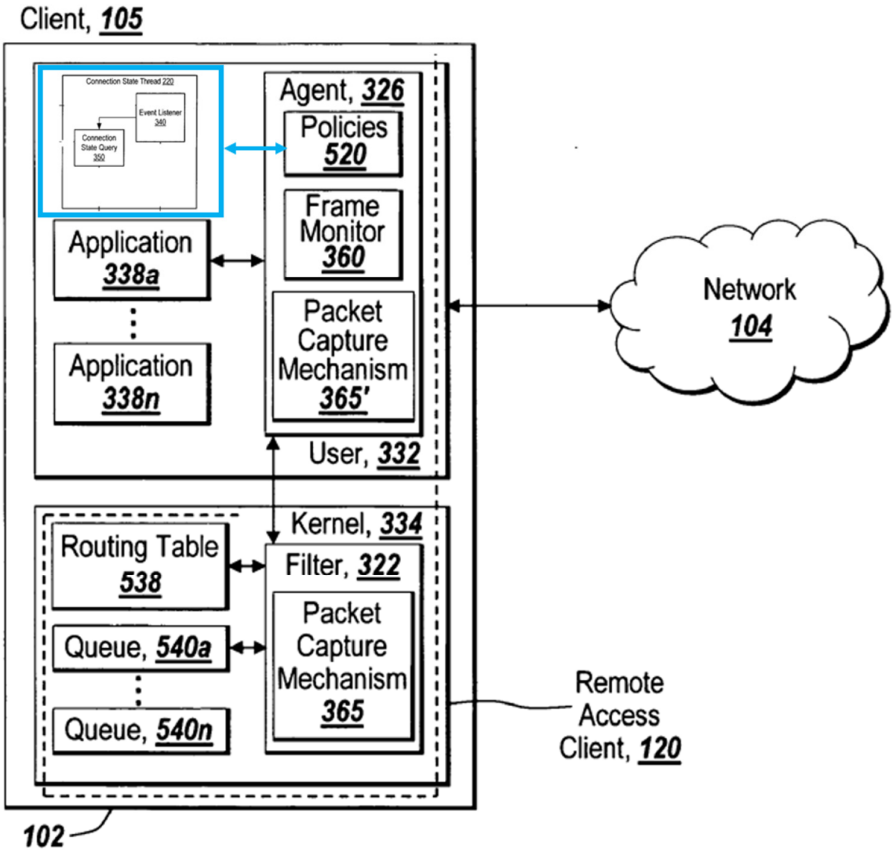
would have recognized that denying an application access to a network is preferable to prioritization since denying both preserves device resources and improves user experience. SAMSUNG-1003, ¶[130].

Therefore, a POSITA would have recognized the benefit of two complementary approaches for managing contention: (1) network prioritization (as taught by Rao) when sufficient bandwidth exists and (2) denying network access to some applications (as taught by Jones) to manage insufficient bandwidth and network contention. SAMSUNG-1005, [0184]; SAMSUNG-1006, 5:13-32; SAMSUNG-1003, ¶[131]. Consequently, a POSITA would have been motivated to combine the teachings of Rao and Jones to operate in instances where bandwidth is limited and there is contention among applications for bandwidth. SAMSUNG-1003, ¶[131].

The resulting Rao-Jones device (RJD) evaluates policies relating to a wide range of factors such as characteristics of the network (e.g., "type of connection, connection bandwidth, user priorities, etc.," per Jones, and "the name of the application, "the type of application," "whether an application is running in the foreground or the background," etc., per Rao. SAMSUNG-1005, [0182], SAMSUNG-1006, 5:13-15; SAMSUNG-1003, ¶[132]. The result of the policy evaluation first determines whether the transfer is allowed (per Jones), and if so, assigns the corresponding packets to a priority-based queue (per Rao). SAMSUNG-1005, [0182], [0189], SAMSUNG-1006, 5:15-32, SAMSUNG-1003, ¶[132]. Therefore, RJD blocks an application's access to the network when

permitting access by the application degrades overall device performance, and for traffic that is permitted, uses the prioritization techniques of Rao. SAMSUNG-1003, ¶[132].

RJD includes Rao's client 105 modified to include the "Connection State Thread" of Jones, as illustrated below. SAMSUNG-1005, FIG. 5A; SAMSUNG-1003, ¶[133].




SAMSUNG-1005, FIG. 5A (modified)

Additionally, RJD can access multiple networks, as taught by Jones, and "rules may be applied to data transfers depending on the ... type of connection," and "policies for data ... are sensitive to the type of connection." SAMSUNG-

1006, 5:13-19; SAMSUNG-1003, ¶[134]. RJD communicates directly or via a gateway with various networked systems, such as other instances of RJD, servers and server farms, as illustrated below. SAMSUNG-1005, [0089]-[0092]; SAMSUNG-1003, ¶¶[135]-[136].

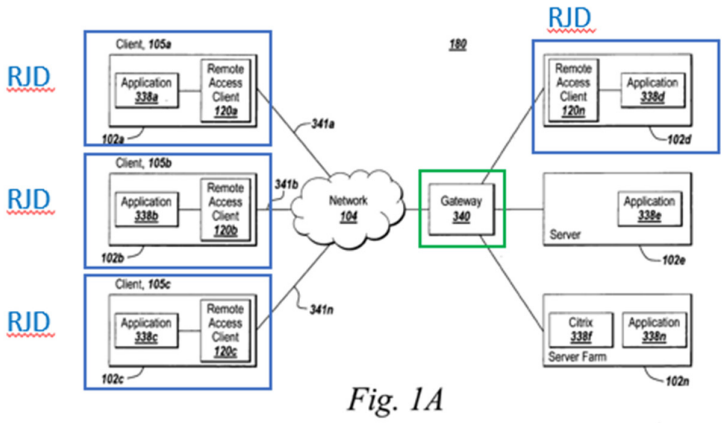



*Fig. 1A*

SAMSUNG-1005, FIG. 1A (modified)

In operation, the RJD client monitors the connection state using the connection state thread (as taught by Jones), which provides the connection state to the policies component 520 (which is analogous to the policy selection component of Jones). SAMSUNG-1006, 4:43-45; SAMSUNG-1003, ¶[137]. The policy component uses the configured policies to determine whether to permit or prevent the data transfer based on the connection state. SAMSUNG-1003, ¶[137]. For permitted data transfers, the RJD client uses the policies to apply a priority to network packets in accordance with the configured policies and queues the packets according to the priority, restricting some packets in favor of

others. SAMSUNG-1005, [0189], [0191], SAMSUNG-1003, ¶[137]. The client then communicates the packets according to the priorities. SAMSUNG-1005, [0194]; SAMSUNG-1003, ¶[137].

Thus, the components of RJD each operate as they would in isolation. SAMSUNG-1003, ¶[138]. A POSITA would have a reasonable expectation of success in creating a combination, which would have required only routine programming knowledge well within the skill of a POSITA. *Id.* Indeed, the change would have amounted to nothing more than the use of a known technique to improve similar mobile devices in a similar way and combining prior art elements according to known methods to yield the predictable results described above. *Id.*; *KSR*, 550 U.S. at 417.

RJD's processor would be configured to perform or assist in performing the operations discussed in this Ground. SAMSUNG-1003, ¶[139].

**2. Analysis**

***[4]***

RJD renders [4] obvious. SAMSUNG-1003, ¶¶[314]-[317].

RJD evaluates policies relating to factors including "whether an application is running in the foreground or the background." SAMSUNG-1005, [0182]; §III.A.1.a SAMSUNG-1003, ¶[315]. The first application can be a non-interactive application such as video streaming (Rao) or backup (Jones). SAMSUNG-1005, [0088], [0179]; SAMSUNG-1006, 5:13-32. SAMSUNG-1003, ¶[315]. The result of RJD's policy evaluation first determines if the transfer is

allowed or prohibited. SAMSUNG-1006, 5:25-26; §III.A.1.a; SAMSUNG-1003, ¶[315]. Thus, RJD prevents network access when the application runs as a background process. SAMSUNG-1005, [0182]; SAMSUNG-1006, 5:25-26; §III.A.1.a; SAMSUNG-1003, ¶[315].

For example, Jones teaches that "data protection software ... may execute in the background to perform data backups" and the "[b]ackup frequency ... may depend on ... enterprise policies." SAMSUNG-1006, 3:45-51. A POSITA would have recognized that preventing network access for backup processes (in the background) leaves additional bandwidth for other applications, avoiding cases where background packets are processed in lieu of or "processed ahead of the real-time network packets," as described in Rao. SAMSUNG-1005, [0003]; SAMSUNG-1003, ¶¶[316]-[317].

***[13]***

RJD renders [13] obvious. SAMSUNG-1003, ¶¶[318]-[319].

Rao teaches that policies are configurable by a user by any suitable means e.g., via a UI designed for specifying policies. SAMSUNG-1005, [0183]. Jones similarly teaches that "a user such as a system administrator may configure policies for data transfers." SAMSUNG-1006, 5:15-29. Therefore, a POSITA would have recognized that RJD's configuration mechanism for specifying policies is an instance of network administrator input, as explained in both Rao and Jones. SAMSUNG-1005, [0183]; SAMSUNG-1006, 5:15-29; SAMSUNG-1003, ¶[319].

***[21]***

RJD renders [21] obvious. SAMSUNG-1003, ¶¶[320]-[324].

RJD policies are based on user input, as described in both Rao and Jones. SAMSUNG-1005, [0183]; SAMSUNG-1006, 6:39-41; *see* [1.7a]; SAMSUNG-1003, ¶[321].

Further, in RJD, the aspect of a control policy (e.g., a clause in the condition) is based, at least in part, on a characteristic of the first or second wireless network. SAMSUNG-1003, ¶[322]. For example, Jones teaches that policies may be applied to data transfers based on connection bandwidth, explaining that "[a] variety of rules may be applied to data transfers depending on ... connection bandwidth ... etc." SAMSUNG-1006, 5:13-15; SAMSUNG-1003, ¶[322]. A POSITA would have recognized bandwidth to be a characteristic of a network. SAMSUNG-1003, ¶[322](citing SAMSUNG-1038). A POSITA would have recognized or found obvious that the condition aspect can depend on multiple factors, e.g., the application name and connection bandwidth, each of which assists in restricting or preventing network access. SAMSUNG-1003, ¶[323].

RJD policies restrict (per Rao) or prevent (per Jones) access to the network. SAMSUNG-1005, [0184]; SAMSUNG-1006, 5:13-32; SAMSUNG-1003, ¶[324]; §III.C.1.b.

***[23]***

RJD renders [23] obvious. SAMSUNG-1003, ¶¶[325]-[328].

RJD supports multiple policies relating to an application. SAMSUNG-

1003, ¶[326]. For example, Rao explains that the remote access client "may have one or more policies" specifying prioritization which can be "based on application, name, protocol, etc." SAMSUNG-1005, [0182]; SAMSUNG-1003, ¶[326]. Jones further teaches that policies can depend on functionality, connection type, connection bandwidth, user priorities, etc., and that a system administrator may configure policies for backups and updates. SAMSUNG-1006, 5:13-19. A POSITA would have recognized that applications (e.g., video streaming, backup and update) would be subject both to rules specified based on application name, etc., and to rules based on functionality, connection type, connection bandwidth, etc., and therefore to multiple (first and second control) policies. SAMSUNG-1005, [0182]; SAMSUNG-1006, 5:13-19; SAMSUNG-1003, ¶[326].

In Rao, such policies control access to networks (including a third access to a second wireless network by RJD, which can access multiple networks) by applications (including the first application, video streaming), e.g., by prioritizing access. SAMSUNG-1006, 5:13-19; §III.C.1.b; s*ee* [1.7b], [1.8], [20]; SAMSUNG-1003, ¶[327].

In RJD, memory stores policies (including a second control policy associated with the first application) and machine-executable instructions executed by processor(s) cause the processor(s) to apply policies (including the second control policy). *See* §III.A.1.a, [1.4]-[1.5]; SAMSUNG-1003, ¶[328].

***[25]***

RJD renders [25] obvious. SAMSUNG-1003, ¶¶[330]-[336].

RJD is capable of being communicatively coupled to a gateway (intermediate networking device) over the first wireless network, as taught by Rao, such that the gateway provides a connection between clients and computing devices. SAMSUNG-1005, [0087], [0095]; §III.C.1.b; SAMSUNG-1003, ¶[330].

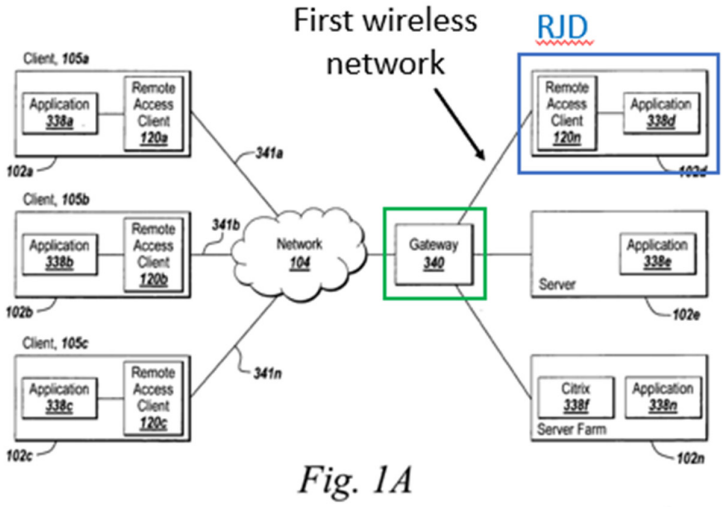



*Fig. 1A*

SAMSUNG-1005, FIG. 1A (annotated)

The gateway provides a forwarding service for forwarding traffic between the wireless device and network systems coupled to the gateway over a second wireless network. SAMSUNG-1005, [0089]-[0092]; SAMSUNG-1003, ¶¶[331]-[333].

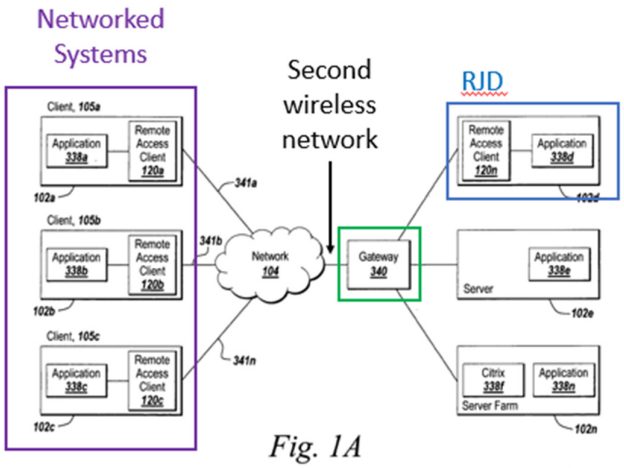



*Fig. 1A*

SAMSUNG-1005, FIG. 1A (annotated)

RJD determines an aspect of the control policy (e.g., a clause in the condition) based on a characteristic (bandwidth) of the second wireless network. SAMSUNG-1003, ¶[334]. For example, Jones explains that "rules may be applied to data transfers depending on ... connection bandwidth." SAMSUNG-1006, 5:13-15. A POSITA would have recognized that the bandwidth available to RJD is the minimum bandwidth of any network between RJD and the communication endpoint with which it is communicating. SAMSUNG-1003, ¶[335]. Therefore, at least when the second wireless network has lower bandwidth than the first wireless network (and therefore limits the end-to-end bandwidth), RJD determines at least an aspect of the control policy based on a characteristic of the second wireless network (bandwidth). SAMSUNG-1003, ¶[336].

### D. Ground 1D: Rao-Jones-Jajoo renders claim 17 obvious

#### 1. Rao-Jones-Jajoo

##### (a) Jajoo

Jajoo describes "controlling data traffic in a wireless or other communication network" where "agents monitor ... layers of the network for the presence of indicators associated with network failover operations." SAMSUNG-1010, Abstract. Based on detected indicators, "the agents determine if a failover operation has occurred"; if so, "data congestion associated with the failover operation is controlled according to a failover congestion monitoring and recovery mode." *Id*.

Jajoo "differentiates between failover congestion and actual congestion" and "[h]ow the traffic is controlled in either case can be both implementation-dependent and traffic-type dependent" such that "different traffic types can be subjected to a reduction/shredding process, and/or to a delay process, and/or to a dropping process." SAMSUNG-1010, [0017]. Jajoo determines failover by evaluating conditions, e.g., by comparing the failover indicators to "empirically determined conditions, criteria, or thresholds." SAMSUNG-1010, [0025].

"[D]ata packets associated with the failover congestion are controlled using the failover congestion control mode" which "accounts for the temporary nature of the failover data congestion," e.g., "failover congestion may be controlled" by delaying "transmission and/or re-transmission of the data packets at the transmission source(s)." SAMSUNG-1010, [0028]. Consequently, "instead

of dropped calls, data packets are delayed in a controlled manner," which "is sufficient to accommodate the failover operation, wherein once the failover operation is complete, the data packets are then transmitted or re-transmitted over the newly established link." *Id*. Additionally, "[t]raffic patterns can be separated ... by adopting an alternate de-queuing algorithm while the failover congestion lasts." *Id.*, [0029].

To determine whether failover has occurred, the network can be monitored for alarms generated by network entities. SAMSUNG-1010, [0009].

(b) **Combination**

Jones describes applying rules based on connection type and bandwidth. SAMSUNG-1006, 5:14-15. A POSITA would have recognized that available bandwidth provided by a network can either be largely permanent (e.g., based on physical properties of the connection) or transient (e.g., when error conditions arise). SAMSUNG-1003, ¶¶[144]-[145].

Additionally, Jajoo teaches that available network bandwidth can vary in response to failover. SAMSUNG-1010, [0006]; SAMSUNG-1003, ¶[146]. For example, Jajoo teaches that when network failover occurs, the result can be "decreased bandwidth and a perceived congestion condition," but since the "network normally handles congestion by dropping the load at the source, failover operations may result in dropped calls," which negatively impacts users. SAMSUNG-1010, [0006]. Instead, Jajoo considers the source and nature of the fail-

over congestion "to reduce instances of dropped calls that would otherwise occur if the failover congestion were handled" conventionally. SAMSUNG-1010, [0007]; SAMSUNG-1003, ¶[147]. Thus, in Jajoo, "data packets associated with the failover data congestion are controlled in a manner that accounts for the temporary nature of the failover data congestion," e.g., "data packets are delayed in a controlled manner until the failover operation is finished." SAMSUNG-1010, [0011]; SAMSUNG-1003, ¶[147]. Therefore, to mask the errors and avoid unnecessary disruption (e.g., multimedia transmission failures such as dropped VoIP calls) caused by failover, a POSITA would have been motivated to modify the RJD with Jajoo's failover monitoring. SAMSUNG-1010, [0007]; SAMSUNG-1003, ¶¶[147]-[148].

In operation, when the client of the resulting Rao-Jones-Jajoo Device (RJJD) recognizes an event, per Jones, it fetches the current state of network interface and forwards the current connection state to the policy selection component. SAMSUNG-1006, 4:40-48; SAMSUNG-1003, ¶[149]. To determine a policy-based response, the RJJD policies determine whether the situation is transient, e.g., as the result of a failover (per Jajoo), by comparing failover indicators to a threshold. SAMSUNG-1010, [0007]-[0010], [0017], [0025], [0029]; SAMSUNG-1003, ¶[149]. Using both the current network condition, and a determination as to whether the situation is transient, RJJD permits or denies access to the network (per Jones), and if access is permitted in the presence of a

transient situation, failover data congestion is controlled accounting for the temporary nature of the failover data congestion using the priority-based queuing of Rao, e.g., by assigning such traffic to a lower-priority queue during the temporary disruption. SAMSUNG-1005, [0179]-[0195]; SAMSUNG-1010, [0011]; SAMSUNG-1003, ¶[149]. As a result, while the multimedia session might suffer temporarily (e.g., stuttering video), the session will not terminate. SAMSUNG-1010, Abstract [0007]-[0008]; SAMSUNG-1003, ¶[149].

Such RJJD policies are based on user input, as described in both Rao and Jones. SAMSUNG-1005, [0183]; SAMSUNG-1006, 6:39-41; §III.C.1.b; SAMSUNG-1003, ¶[149].

**2. Analysis**

***[17]***

RJJD renders [17] obvious. SAMSUNG-1003, ¶¶[337]-[342].

RJJD policies contain a condition aspect and an action aspect. *See* [1.7a]. RJJD policies are based on user input, as described in both Rao and Jones. SAMSUNG-1005, [0183]; SAMSUNG-1006, 6:39-41; §III.D.1.b; SAMSUNG-1003, ¶[338]. Therefore, it would have been obvious to a POSITA that since a policy includes condition and action aspects, the condition aspect and the action aspect of the policy are based on user input. SAMSUNG-1003, ¶[338](citing SAMSUNG-1032, SAMSUNG-1039).

In the case where a second network fails over to a first network, RJJD policies evaluate the behavior of networks (e.g., a second wireless network),

e.g., using network failover indicators, thereby determining failover from the second network to the first network by evaluating metrics of the second network. SAMSUNG-1010, Abstract, [0009], [0025]; SAMSUNG-1003, ¶¶[339]-[340]. Thus, it would have been obvious to a POSITA to include, in RJJD's policies, conditions that compare the failover indicators to "conditions, criteria, or thresholds associated with failover operations in the network." SAMSUNG-1003, [341]; SAMSUNG-1010, [0025].

When a failover from a second network to a first network is detected, the conditions of an RJJD policy evaluate to TRUE, and a corresponding action is selected. SAMSUNG-1003, ¶[342]. The selected policy action controls traffic using a "delay process" (per Jajoo) for traffic from the first application (video streaming, per Rao). SAMSUNG-1005, [0088]; SAMSUNG-1010, [0017]; SAMSUNG-1003, ¶[342]. RJJD implements the delay using Rao's priority queues, e.g., via policy actions that assign a lower priority to the packets, which results in the packets being placed in lower-priority queues, thereby delaying packet transmission. SAMSUNG-1005, [0179]-[0195]; SAMSUNG-1003, ¶[342].

### E. Ground 1E: Rao-Jones-Cole renders claim 22 obvious

#### 1. Rao-Jones-Cole

##### (a) Cole

Cole is directed to providing network connectivity for a mobile device with multiple "communication interfaces." SAMSUNG-1029, Abstract. Figure

1 (below) shows a mobile device connected to WWAN and WLAN networks. SAMSUNG-1003, ¶[151]; SAMSUNG-1029, [0031].

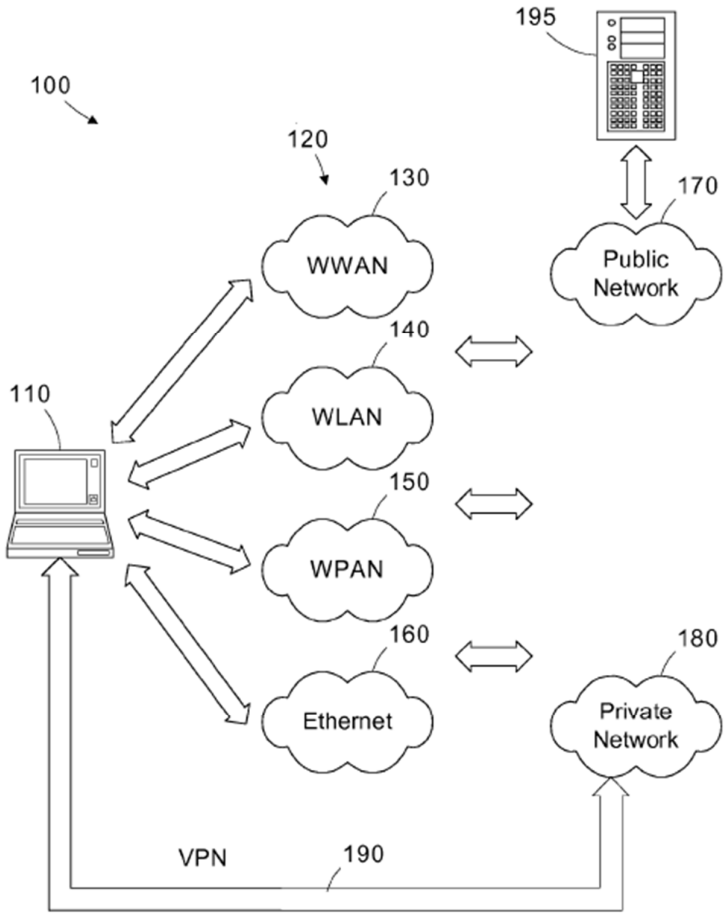



**Figure 1**

SAMSUNG-1029, FIG. 1

Cole addresses situations where the bandwidth being used on a connection approaches a bandwidth limit, causing performance of the device and its applications to degrade. SAMSUNG-1029, [0073]. For example, "if the con-

nection is being used nearly to capacity and an additional application is executed that requires still more bandwidth, the connection may not be able to support the total load" so "running applications may experience increased latency for data transfers." *Id.* In response, Cole's connection manager "tries to proactively prevent increased latency from an overloaded connection from impacting the performance of the running applications or the efficiency of the user." *Id.*, [0074].

In response, "[w]hen the monitored load exceeds a predetermined threshold" the connection manager can manage the load by "attempt[ing] to establish a connection with a higher bandwidth," e.g., attempting to connect to a network with higher capacity. SAMSUNG-1029, [0075], [0077].

To select a network interface, the connection manager evaluates availability, bandwidth, user preferences, etc. SAMSUNG-1029, [0036]. The connection manager identifies "available connections and uses the default hierarchy to select a particular communication interface." *Id.*, [0045]. While an example default hierarchy can be "LAN, WLAN, WWAN, WPAN," the user can override the default hierarchy by setting preferences or selecting particular networks that may or may not be used." *Id.*, [0042], [0067]. Thus, Cole's connection manager establishes connectivity "to the fastest eligible connection based on the connection time data and the user's preferences." *Id.*, [0067]

(b) **Combination**

Jones describes applying rules based on "type of connection, connection

bandwidth, [and] user priorities." SAMSUNG-1006, 5:14-15. A POSITA would have recognized that while total bandwidth of a connection is relevant, also relevant is the bandwidth available at a given time. SAMSUNG-1003, ¶[155]. Consequently, a POSITA would have looked to references such as Cole, which teaches determining whether monitored load exceeds a predetermined threshold. SAMSUNG-1029, [0075]; SAMSUNG-1003, ¶[155]. A POSITA would have recognized that, by monitoring currently-available bandwidth, and seeking better connections when such bandwidth fails to satisfy the device's needs, the device can ensure that the available bandwidth supports the demands of applications running on the device. SAMSUNG-1029, [0075], [0077]; SAMSUNG-1003, ¶[155].

In operation, when the resulting Rao-Jones-Cole Device (RJCD) determines that available bandwidth fails to satisfy a threshold, the device uses control policies relating to connection order (per Cole) to select a network with higher-bandwidth. SAMSUNG-1029, [0036], [0045], [0075], [0077]; SAMSUNG-1003, ¶[156]. Such control policies relating to connections are based on user preferences (which determine connection order policies). SAMSUNG-1029, [0042], [0067]; SAMSUNG-1003, ¶[156]. RJCD uses the techniques of Jones to determine whether a particular transfer is permitted over a connection, and if so, uses the priority-queueing techniques of Rao to manage use of the connection bandwidth. SAMSUNG-1005, [0184]; SAMSUNG-1006, 3:55-67; SAMSUNG-1003, ¶[156].

**2. Analysis**

***[22]***

RJCD renders [22] obvious. SAMSUNG-1003, ¶¶[343]-[346].

RJCD policies, which include packet priorities, are "configurable by a user," thereby reflecting a user preference. SAMSUNG-1005, [0183]; *see* [9]; SAMSUNG-1003, ¶[344]. Similarly, Cole teaches control policies for selecting connections that direct RJCD to attempt "to establish connectivity to the fastest eligible connection based ... ***the user's preferences***." SAMSUNG-1029, [0067]. Such control policies alter the default connection order, e.g., when a user "select[s] particular networks that may or may not be used." *Id.*; SAMSUNG-1003, ¶[344].

Cole further teaches that policies, which are based on user preferences (as described immediately above), are directives to allow access to a second wireless network based on a characteristic of the first network. SAMSUNG-1003, ¶[345]. Cole provides a first example in which the device "is connected to the remote network through the first communication interface" (first network), but in response to a "loss of connectivity" (characteristic of that network), a "second one of the communication interfaces is selected for establishing a second connection to a remote network" (second network). SAMSUNG- 1029, Abstract; SAMSUNG-1003, ¶[345]. In this case, the condition aspect includes a "loss of connectivity" clause in the condition's Boolean expression. SAMSUNG-1003,

¶[345]. Cole provides a second example in which "the monitored load [characteristic of the first network] exceeds a predetermined threshold," and in response, the connection manager attempts "to establish a connection [to a second network] with a higher bandwidth." SAMSUNG-1029, [0075], [0077]; SAMSUNG-1003, ¶[345]. Here the condition aspect includes a bandwidth threshold (of the first network) clause in the condition's Boolean expression. SAMSUNG-1003, ¶[345].

### F. Ground 1F: Rao-Montemurro renders claim 5 obvious

#### 1. Rao-Montemurro

##### (a) Montemurro

Montemurro describes communication devices "capable of at least two communication modes," e.g., WLAN and WWAN, that optimize communications using a policy to configure connections and routes. SAMSUNG-1008, Abstract. A "rules engine evaluates its policies on a state change ... to configure a routing table" and "provides an appropriate connection to an application for its respective communications." *Id.* Policies are responsive to various factors (e.g., bandwidth, application type). *Id.*

Montemurro describes a policy where the MP3 download application runs on the "lowest cost network" available. SAMSUNG-1008, [0029]. In another example, "the CRM application ... only synchronizes the sales contact database" over a WLAN network. *Id.*

Figure 2 (below) shows a device configured with Montemurro's system. SAMSUNG-1008, [0025]-[0037].

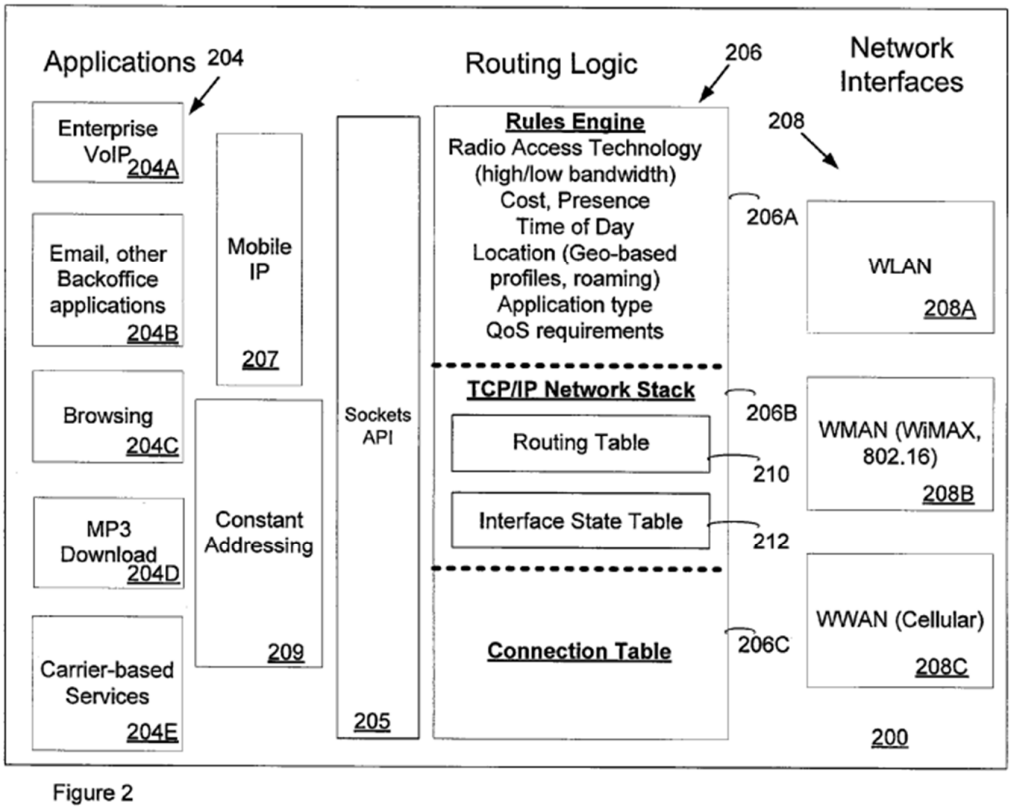


Figure 2

SAMSUNG-1008, FIG. 2

(b) **Combination**

As described above, Rao manages network access using priority-based queues. *See* §III.A.1.a. A POSITA would have recognized that, when a device has multiple network interfaces, further efficiency is gained by assigning different applications to different networks, e.g., the examples from Montemurro, where the MP3 download application runs on the lowest cost network and "the CRM application ... only synchronizes the sales contact database ... over a WLAN network." SAMSUNG-1008, [0029]; SAMSUNG-1003, ¶[163]. Thus,

to improve efficiency of RD, a POSITA would have looked to teachings of other references, such as Montemurro. SAMSUNG-1003, ¶[163].

In operation, the resulting Rao-Montemurro Device (RMD) (i) uses the techniques of Montemurro to select the most appropriate network for an application, and (ii) uses Rao's priority queuing to manage network access. *See* §III.A.1.a; SAMSUNG-1008, Abstract; SAMSUNG-1003, ¶[164].

#### 2. Analysis

***[5]***

RMD renders [5] obvious. SAMSUNG-1003, ¶¶[347]-[349].

RMD can access a first wireless network that is a cellular network. SAMSUNG-1003, ¶¶[348]-[349]. For example, Montemurro explains that in an example network, the mobile device "is capable of wireless communication in accordance with WLAN or ... WWAN (e.g. GSM Cellular) standards," and "[a]s such, it may communicate through [the] cellular network." SAMSUNG-1008, [0013].

### G. Ground 1G: Rao-Akhtar renders claim 7 obvious

#### 1. Rao-Akhtar

##### (a) Akhtar

Akhtar explains that "[a]pplications using wireless technology for data delivery have to explicitly reserve network resources ... to meet unique resource requirements for the content being transmitted." SAMSUNG-1009, [0016]. Such reservation must "be done by the originating and terminating parties for

satisfactory communication since various media content have specific requirements in terms of delay and jitter tolerance," which can be characterized as "delay sensitive, rate sensitive, time sensitive, or some other quality adversely impacting the communication." *Id.*

In response, Akhtar teaches a communication protocol that allocates network resources where a "radio network controller maintains quality of service (QoS) profiles." SAMSUNG-1009, Abstract. Akhtar is "aimed toward reserving resources to support communications between" access devices ("access terminals") that are "IP based." *Id.*, [0028].

In Akhtar, a radio network controller "sets aside resources a priori for the terminating end without waiting for a request" from the terminating access terminal. SAMSUNG-1009, [0017]. To accomplish resource reservation, "[a] serving node determines the type of application ... and determines a QoS policy it transmits to the radio network" and "[t]he radio network identifies the QoS profile based on the received policy and allocates network resources before announcing the call to an access terminal." *Id.*, Abstract.

(b) **Combination**

Rao's RAC "controls network communication prioritizations on the client" where the prioritizations are based on priorities of the client applications. SAMSUNG-1005, [0080]. Such network communication is "generally described in connection with an internet protocol (IP) based protocol." SAMSUNG-1005, [0082].

A POSITA would have recognized that Rao's client-side prioritization is insufficient to achieve end-to-end communication network requirements. SAMSUNG-1003, ¶¶[171]-[173]. As a result, as Akhtar explains, "[a]pplications using wireless technology for data delivery have to explicitly reserve network resources." SAMSUNG-1009, [0016].

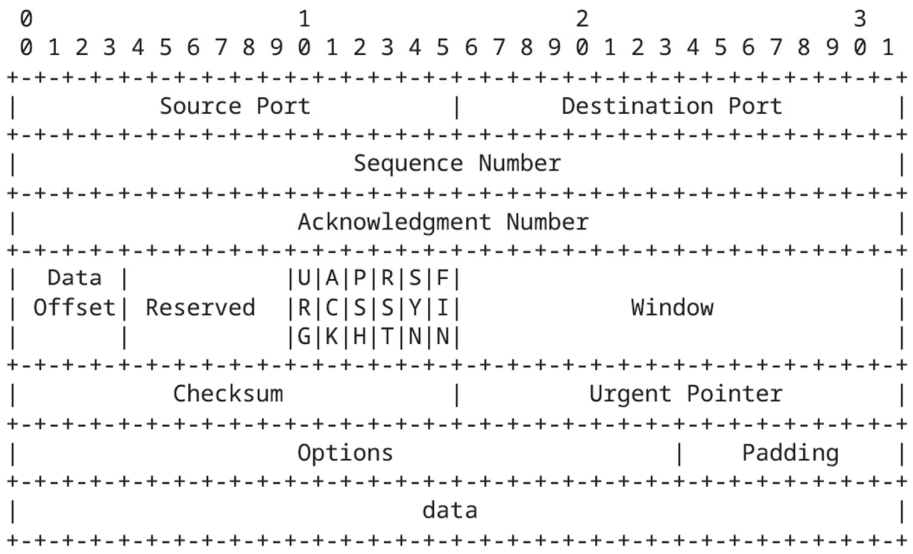
Consequently, a POSITA would have been motivated to implement RD's RAC as a terminal device in Akhtar's wireless communication network, creating the Rao-Akhtar Device (RAD) in which applications reserve network resources (per Akhtar), and when RAD transmits data, packets are sent according to Rao's application-aware prioritization. SAMSUNG-1005, [0179]-[0195]; SAMSUNG-1003, ¶[174]. In the resulting system, packets leave RAD according to priority (per Rao) and are processed by the intermediate network according to the appropriate QoS profile (per Akhtar). SAMSUNG-1003, ¶[174].

**2. Analysis**

***[7]***

RAD renders [7] obvious. SAMSUNG-1003, ¶¶[350]-[360].

Rao teaches using TCP/IP, which a POSITA would have known includes a source port in the header. SAMSUNG-1005, [0095]; SAMSUNG-1003, ¶¶[351]-[352](citing SAMSUNG-1026).




SAMSUNG-1026, FIG. 3

A POSITA would have further known that TCP source ports are associated with applications. SAMSUNG-1003, ¶[355](citing SAMSUNG-1027). A POSITA would have known that the TCP header, including the source port, is preserved until it reaches its destination, and thus preserves the association of the traffic flow (packet) with the first application when the traffic flow is processed by the wireless device. SAMSUNG-1003, ¶¶[355]-[358].

RAD identifies the application (e.g., VoIP) "associated with the transmitted data" based on characteristics of the incoming data packets, including "the source IP address, the destination IP address ... source port number, destination port number," etc. SAMSUNG-1009, [0028]; SAMSUNG-1003, ¶[359].

Thus, in RAD, applying a policy includes identifying a flow tag associated with the application (source port), where the flow tag preserves the associa-

tion of the traffic flow with the first application when the traffic flow is processed by functions of the wireless device that operate on the traffic flow (the TCP network stack in RAD), which is required for Akhtar's QoS. SAMSUNG-1009, Abstract, [0028]; §III.G.1.b; SAMSUNG-1003, ¶[360].

## H. Ground 1H: Rao-Ramesh renders claim 18 obvious

### 1. Rao-Ramesh

#### (a) Ramesh

Ramesh explains that "the next-generation distributed computing environment ... may have a large number of roaming mobile nodes/devices." SAMSUNG-1011, [0001]. However, frequent changes of business requirements can require rapid re-configuration of security parameters in mobile devices. *Id.*, [0004].

Ramesh's disclosure provides "policy-managed communities of interest" in which "assets may be kept under the control of a policy manager" and "assets may be protected so that they respond only to requests from subjects based on the approval of entitlement-specifying policies." SAMSUNG-1011, [0021].

In Ramesh, a policy distribution node (PDN) distributes policies to policy decision points on mobile clients (MCs) via a policy exchange channel (PXC). SAMSUNG-1011, [0036]. Since not all MCs carry security policies, a PDN can distribute the appropriate set of security policies to MCs based on their access control identities and roles. SAMSUNG-1011, [0036]. Ramesh further

explains that the PXC may provide a secure protocol that allows policy distribution from the PDN to the PDP through the PEP, e.g., using existing industry standards such as TLS and SSH FTP secure extension. SAMSUNG-1011, [0037].

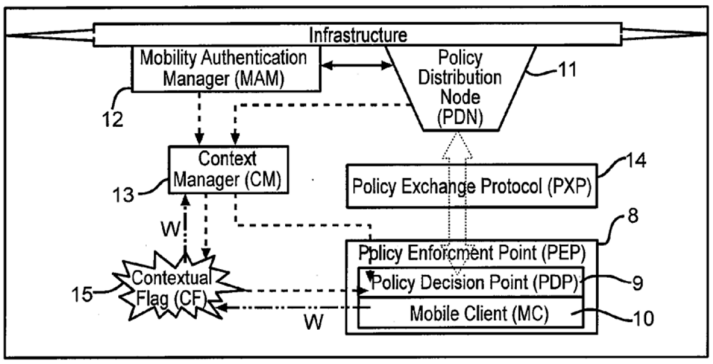



FIG. 3

SAMSUNG-1011, FIG. 3

(b) **Combination**

Rao teaches that policies can be "loaded by the agent." SAMSUNG-1005, [0183]. For example, Rao explains that the "policies may be provided by or downloaded via the gateway," an example of a network element. *Id.*; SAMSUNG-1003, ¶[181]. A POSITA would have recognized that policy distribution from Ramesh's PDN to a mobile client (as taught by both Rao and Ramesh) is an example of a policy being "loaded by the agent," as taught by Rao. SAMSUNG-1003, ¶[181]. Therefore, a POSITA would have been motivated to modify RD with Ramesh's teaching of secure policy distribution to prevent tampering with policies during distribution. SAMSUNG-1003, ¶[181]. In the result-

ing Rao-Ramesh Device (RRD), secure policy distribution advantageously prevents policy tampering, e.g., where "[c]ompromised data content may potentially lead to fatal consequences." SAMSUNG-1011, [0024]; SAMSUNG-1003, ¶¶[181]-[182].

In RRD, policies can be configured into the device (e.g., as taught by Rao) and/or downloaded from a network element (PDN) over a secure link (as taught by Ramesh). SAMSUNG-1005, [0183]; SAMSUNG-1003, ¶¶[182]-[183].

**2. Analysis**

***[18]***

RRD renders [18] obvious. SAMSUNG-1003, ¶¶[361]-[367].

Ramesh includes a PDN that distributes polices to devices via a PXC. SAMSUNG-1011, [0036]; SAMSUNG-1003, ¶[362]. Since the PDN distributes policies to devices, RRD obtains policies from the PDN. SAMSUNG-1003, ¶[362]. Since Rao teaches that the policies may be provided by the gateway, a POSITA would have recognized that Rao's gateway (which is a network element) is serving as a PDN. SAMSUNG-1005, [0183]; SAMSUNG-1003, ¶[362]. More generally, since PDNs are connected to RRDs over a network, a POSITA would have recognized that Ramesh's policy distribution node is a network element. SAMSUNG-1003, ¶[362].

In RRD, the control link (PXC) is secured by an encryption protocol, e.g., TLS. SAMSUNG-1011, [0037]; SAMSUNG-1003, ¶[363]. Ramesh explains

that the Policy Exchange Channel (PXC) can provide a secure protocol allowing distribution of policies from PDN to PDP 9 through PEP 8, e.g., using encrypted protocols such as TLS and SSH FTP secure extension. SAMSUNG-1011, [0037]; SAMSUNG-1003, ¶[363]. A POSITA would have recognized that control links using encrypted protocols (e.g., TLS) are secured by an encryption protocol. SAMSUNG-1003, ¶[363](citing SAMSUNG-1021). Additionally, a POSITA would have recognized that since the control link "allow[s] the distribution of policies," and policies are used to manage communication sessions, the control link supports control-plane communications between the wireless device and the network element. SAMSUNG-1011, [0037]; SAMSUNG-1003, ¶[364]; *see* SAMSUNG-1053, 3.

Further, a POSITA would have known that clients (e.g., RRD) assist in establishing TLS links using a handshake protocol. SAMSUNG-1003, ¶[365](citing SAMSUNG-1021).

Therefore, RRD assists in establishing a secure control link (e.g., TLS handshake) secured by an encryption protocol and obtaining control policies from the network element over the secure control link (from Ramesh's PDN). SAMSUNG-1011, [0036]-[0037]; SAMSUNG-1003, ¶[366].

Machine-executable instructions cause RRD's processor to perform the operations. §III.A.1.a; SAMSUNG-1003, ¶[367].

## I. Ground 1I: Rao-Freund renders claims 12, 15-16, 26-27, and 29-30 obvious

### 1. Rao-Freund

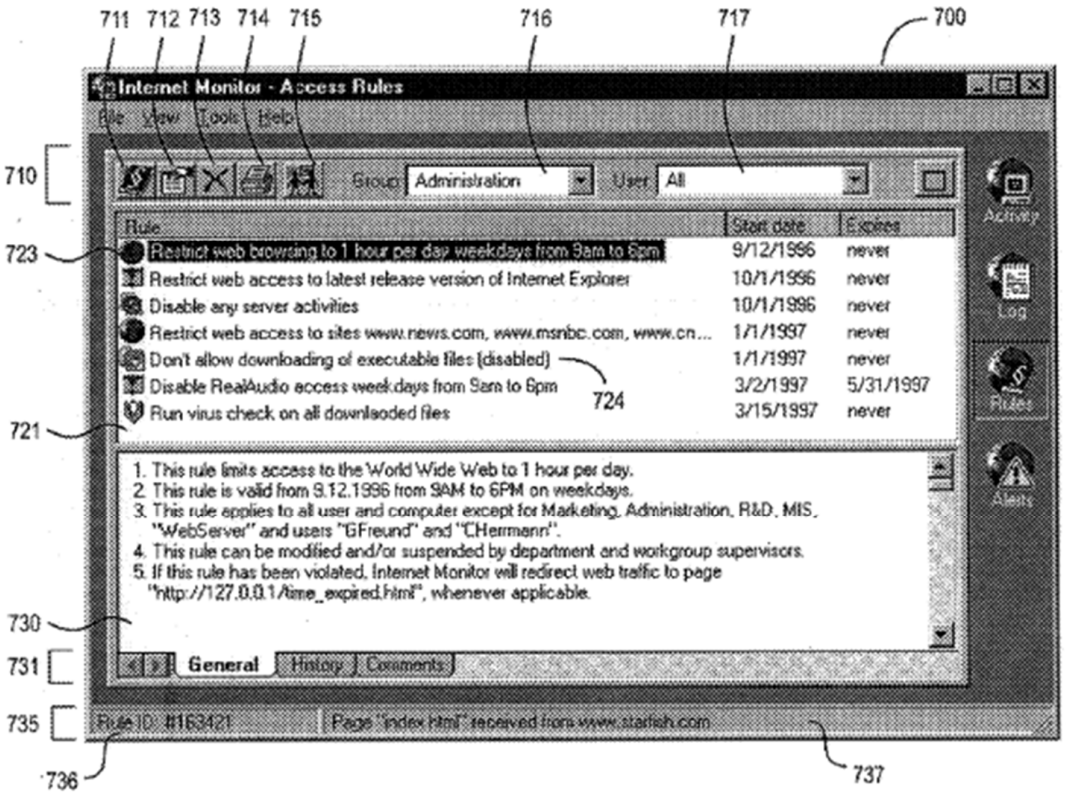
#### (a) Freund

Freund addresses challenges, including "ho[a]rding available network bandwidth through use of bandwidth-intensive applications (e.g., real-time audio programs)." SAMSUNG-1013, 2:12-14. For example, Freund's system monitors "access to the Internet by individual applications" which "allows the system ... to not only track Internet traffic" but also "determine in many cases data exchanged on a per application basis." *Id.*, 11:9-15. "[P]er application monitoring simplifies the task of tracking bandwidth utilization for a network, including providing detailed review on how the Internet access is being used" which "greatly eases planning of hardware and connection requirements." *Id.*, 11:20-25. Additionally, "[i]nadvertent disruptions of the network by individual users, such as bandwidth ho[a]rding by a user using RealAudio for listening to a Web audio 'broadcast,' can be averted." *Id.*, 11:25-28.

To address such issues, Freund uses "access rules" for efficient use of computing resources and controlling the use of networks. SAMSUNG-1013, 3:62-67; SAMSUNG-1003, ¶[187]. "[A]ccess rules can include criteria such as total time a user can be connected to the Internet," "time a user can interactively use the Internet," and "a list of applications or application versions that a user can or cannot use in order to access the Internet," among others. SAMSUNG-1013, 4:8-19.

To enforce rules, Freund includes "bandwidth and interactive use monitoring" during which a Client Monitor intercepts networking calls and "[a]dds the data lengths to a DataIn or DataOut accumulator or counter of the Application's list entry and global activity record." SAMSUNG-1013, 30:11-26. The Client Monitor then checks whether "the DataIn or DataOut fields exceed rule-based quantity either for the specific Application or the user/workstation," and if so "the Client Monitor disables future Internet access and/or warns the user." *Id.*, 30:26-29.

To enable rule configuration, "a preferred user interface or 'wizard' dialogs for configuring rules," displays "rules governing operation of the Internet access monitor" and rules that "are available for a current configuration," and allows a user to create, edit, or delete rules. SAMSUNG-1013, 24:16-24. Figure 7A (below) shows an example UI panel.




SAMSUNG-1013, FIG. 7A

Policies are loaded from a network element ("supervisor"), and "the Supervisor filters rules appropriate for the client ... and transmits them to the Client Monitor." SAMSUNG-1013, 28:14-18. The Client Monitor "saves a copy of the rules onto a local hard disk" where they are ready for use. SAMSUNG-1013, 28:18-19.

(b) **Combination**

Rao and Freund describe using policies/rules to control network traffic. For example, as described above, Rao "may apply a policy to determine a condition of the client 105 ... at the time of transmission of the packet." SAMSUNG-1005, [0109]. Further, the frame monitor "may identify an application

338 that generated the packet," and the frame monitor "may make a policy-based determination to transmit the packet to the gateway 340 responsive to the identified application." *Id.* Rao explains such "***policies 520 may be specified by any suitable means and/or mechanisms***," including the name or type of the application, "the type of one or more protocols used by the applications 338a-338n and/or the size of the payload of the network packet," and "whether an application is running in the foreground or the background of the client." *Id.*, [0182]-[0184]. Rao notes that a POSITA "will recognize and appreciate the multitude of ways to define client-side application priorities." *Id.*

A POSITA would have recognized that the network traffic control policies of Freund are simply additional examples of client-side policies, such as those Rao contemplates. SAMSUNG-1003, ¶[192]. For example, Freund includes "access rules [that] can include criteria such as total time a user can be connected to the Internet ... time a user can interactively use the Internet ... a list of applications or application versions that a user can or cannot use in order to access the Internet, a list of URLs (or WAN addresses) that a user application can (or cannot) access, a list of protocols or protocol components ... that a user application can or cannot use" and a "rule-based quantity either for the specific Application or the user/workstation" limiting network data use. SAMSUNG-1013, 4:9-19. 30-26-29. A POSITA would have naturally recognized that Freund's policy examples are among the "multitude of ways to define client-side application priorities" described in Rao and recognized that Freund's policy

examples could be incorporated in Rao. SAMSUNG-1005, [0182]; SAMSUNG-1003, ¶[192].

Rao further teaches that policies "may be configurable by a user by any suitable means and/or mechanism ... such as a user interface, graphical or otherwise, design[ed] and constructed for configuring or specifying the policies." SAMSUNG-1005, [0183]. For details on the UI, a POSITA would have looked to references such as Freund, which shows "bitmap screenshots illustrating a preferred user interface or 'wizard' dialog for configuring rules" including a preferred interface that "provides a 'view' of rules governing operation of the Internet access monitor, displaying all of the rules which are available for a current configuration." SAMSUNG-1013, 6:47-49, 24:17-20, FIGS. 7A-K; SAMSUNG-1003, ¶[193]. Such a UI allows a user to create, edit, or delete rules. SAMSUNG-1013, 24:22-24.

Rao explains that policies "may be accessible by the agent 326, configured into the agent 326, or loaded by the agent 326," e.g., the policies "may be provided by or downloaded via the gateway." SAMSUNG-1005, [0183]. For implementation details on how to obtain the policies, a POSITA would have looked to references such as Freund. SAMSUNG-1003, ¶[194]. As described above, Freund teaches an example of policies being loaded by an agent: "the Supervisor filters rules appropriate for the client (i.e., application, Host, and other rules), and transmits them to the Client Monitor." SAMSUNG-1013, 28:14-18.

Because both Rao and Freund teach using policies/rules to control network traffic, including defining and loading policies/rules, it would have been obvious to a POSITA to combine the teachings of Rao and Cole with Freund's teachings to achieve the benefits of Freund's UI for configuring rules and for more detailed enumeration of network traffic control policies contemplated but not explicitly described in Rao. SAMSUNG-1003, ¶[195].

In operation, the resulting Rao-Freund Device (RFD) would use policy-based traffic management techniques of Rao and Freund to use networks efficiently. SAMSUNG-1005, [0182]-[0183]; SAMSUNG-1013, 4:9-19; SAMSUNG-1003, ¶[196]. Freund's Client Monitor function is included in RFD's RAC. SAMSUNG-1003, ¶[196]. For example, Rao's RAC "transparently intercepts network communications associated with applications executing on the client ... and determines priorities for the network communications based on a priority for the application." SAMSUNG-1005, [0080]. A POSITA would have recognized that RAC's transparent interception can be accomplished using Freund's teaching that an application calls an API (e.g., WinSock send()), and the Client Monitor intercepts the call. SAMSUNG-1013, 30:16-17; SAMSUNG-1003, ¶[196]. RFD adds the data lengths (measure of usage) to a counter associated with the application and uses the counter to apply rules. SAMSUNG-1013, 30:24-29; SAMSUNG-1003, ¶[196].

Additionally, the policies governing the operation of RFD would be configured with the UI techniques of Freund and/or loaded from a network element

using the techniques of Rao and Freund. SAMSUNG-1005, [0182]-[0183]; SAMSUNG-1013, 24:22-24; SAMSUNG-1003, ¶[197].

**2. Analysis**

***[12]***

RFD renders [12] obvious. SAMSUNG-1003, ¶¶[368]-[369].

As taught by Freund, in RFD, to send data, an application (e.g., a video streaming application of Rao) calls an API (e.g., WinSock send()), and the Client Monitor intercepts the call. SAMSUNG-1005, [0088]; SAMSUNG-1013, 30:16-17; SAMSUNG-1003, ¶[369]. RFD adds the data lengths (measure of usage) to a counter associated with the application. SAMSUNG-1013, 30:24-26; SAMSUNG-1003, ¶[369]. RFD then determines whether the counter exceeds a "rule-based quantity" (control policy specifying a usage limit) for the application, and if so, disables future Internet access and/or warns the user. SAMSUNG-1013, 30:26-29; SAMSUNG-1003, ¶[369].

***[15]***

RFD renders [15] obvious. SAMSUNG-1003, ¶¶[370]-[373].

As Freund teaches, RFD adds data lengths (amount of usage) to a counter associated with the application (e.g., Rao's video streaming). SAMSUNG-1005, [0088]; SAMSUNG-1013, 30:24-26; SAMSUNG-1003, ¶[371]. RFD then determines whether the counter exceeds a "rule-based quantity" (control policy specifying condition related to a usage limit threshold) for the application, and

if so, disables (blocks) future Internet access and/or warns the user. SAMSUNG-1013, 30:26-29; SAMSUNG-1003, ¶¶[371]-[372].

In RFD, control policies result from user input. *See* [1.6], [1.7a]; SAMSUNG-1003, ¶[373]. Additionally, Freund teaches a "rule wizard interface" that "allows [a] user (e.g., administrator)" to configure "rules which govern use of the protocols monitored by the system." SAMSUNG-1013, 23:65-24:1.

***[16]***

RFD renders [16] obvious. SAMSUNG-1003, ¶¶[374]-[375].

For example, Freund's wizard dialog (which obtains the user input) "asks the user what kind or type of new rule should be created." SAMSUNG-1013, 25:1-3. Freund's rules are combinations of "access rights granted on the basis of available applications, permitted time limits, permitted user activities, permitted protocols, and the like," which can include an indication of a threshold that defines the permitted data use by an application (as accumulated in the DataOut counter). SAMSUNG-1013, 25:3-6, 30:24-29; SAMSUNG-1003, ¶[375].

***[26]***

RFD renders [26] obvious. SAMSUNG-1003, ¶¶[376]-[377].

As Freund teaches, in RFD, to send data, an application (e.g., video streaming of Rao) calls an API (e.g., WinSock send()), and the Client Monitor intercepts the call. SAMSUNG-1005, [0088]; SAMSUNG-1013, 30:16-17; SAMSUNG-1003, ¶[377]. RFD adds the data lengths of the send (measure

quantifying an access) to a counter associated with the application. SAMSUNG-1013, 30:24-26; SAMSUNG-1003, ¶[377].

***[27]***

RFD renders [27] obvious. SAMSUNG-1003, ¶¶[378]-[379].

As Freund teaches, RFD determines the measure (amount of data sent) quantifying network access by the first application. *See* [26]; SAMSUNG-1013, 30:16-26; SAMSUNG-1003, ¶[379].

***[29]***

RFD renders [29] obvious. SAMSUNG-1003, ¶¶[380]-[383].

As Freund teaches, RFD includes a measure of an amount of data sent (e.g., during a Winsock send()) by the first application (e.g., Rao's video streaming). SAMSUNG-1005, [0088]; SAMSUNG-1013, 30:16-26; SAMSUNG-1003, ¶[381].

Freund further teaches a time measure, explaining that "monitoring the total time particular applications access the Internet provides enhanced control." SAMSUNG-1013, 10:45-45; SAMSUNG-1003, ¶[382]. Freund's monitoring "can track Internet access on a per application basis -- that is, access broken down by the application or applications used for the access," which "affords much better tracking and regulating of Internet activities, and "by monitoring total time users/workstations access the Internet, an organization can better determine the overall Internet access requirements and loads." SAMSUNG-1013, 10:47-54; SAMSUNG-1003, ¶[382].

***[30]***

RFD renders [30] obvious. SAMSUNG-1003, ¶¶[384]-[386].

RFD determines whether the counter exceeds a "rule-based quantity" (control policy specifying condition related to a usage limit threshold) for the application (e.g., Rao's video streaming), and if so, disables (blocks) future Internet access and/or warns the user. SAMSUNG-1005, [0088]; SAMSUNG-1013, 30:26-29; SAMSUNG-1003, ¶[385]. A POSITA would have known that warning a user was conventionally done in a panel of a UI. SAMSUNG-1003, ¶¶[385]-[386].

## J. Ground 1J: Rao-Freund-Bedi renders claim 28 obvious

### 1. Rao-Freund-Bedi

#### (a) Bedi

Bedi explains that "[i]t is impossible to maintain an adequate log file on some pervasive devices, since the required storage space may run to many megabytes and the available storage may quickly fill up." SAMSUNG-1030, [0004]. In response, an apparatus that "includes a publishing capability for transmitting log data ... to a publish/subscribe message broker system" and providing "access to an application's log data that conventionally would be saved" locally, but that "do not have sufficient non-volatile storage capacity to store a large log file locally." *Id.*, [0038]-[0039].

(b) **Combination**

In cases where RFD lacks the resources necessary to evaluate policies, e.g., lacking sufficient storage to evaluate policy conditions, a POSITA would have looked to references such as Bedi, which teaches remote log files for resource-constrained devices. SAMSUNG-1030, Abstract, [0004]; SAMSUNG-1003, ¶[201]. Additionally, a POSITA would have recognized that RFD is a pervasive (mobile) device as taught by Bedi. SAMSUNG-1003, ¶[201]; SAMSUNG-1030, [0004].

In a system including RFD as modified by Bedi, monitoring data are transmitted via a message broker to a subscriber tasked with aggregating quantified monitoring data, and providing the data to a PDP, which can be RFD. SAMSUNG-1003, ¶¶[202]-[204](citing SAMSUNG-1032). The PDP evaluates the policy and provides the decisions (e.g., whether to block the traffic, per Freund) to RFD for enforcement. SAMSUNG-1003, ¶[202]. As a result, the policy-based management provided by RFD can operate even when the overall or available resources (e.g., storage) of RFD are insufficient to support that function. SAMSUNG-1003, ¶[202].

**2. Analysis**

***[28]***

RFD as modified by Bedi renders [28] obvious, SAMSUNG-1003, ¶¶[387]-[389].

As described above, when RFD lacks sufficient storage to collect

measures quantifying access to the network, RFD provides such data to a data aggregator (network element), as described by Bedi. SAMSUNG-1030, [0004], [0038]-[0039]; §III.J.1.b; SAMSUNG-1003, ¶[388]. To enforce policies on applications, including the first application, RFD obtains a measure quantifying network access by the first application from Bedi's data aggregator, and uses that value to enforce the policy. *See* §III.I, §III.J.1.b; SAMSUNG-1003, ¶¶[388]-[389].

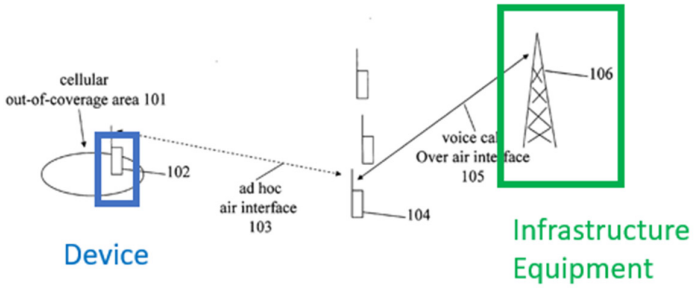
### K. Ground 2: Rao-Pregont-Jones renders claims 1 and 24 obvious

The analysis of Ground 2 is similar to Ground 1, with the exception of the *first application*. In Ground 1, video streaming is provided as an example *first application*; in Ground 2, Pregont's relay application is provided as an example *first application*.

#### 1. Rao-Pregont-Jones

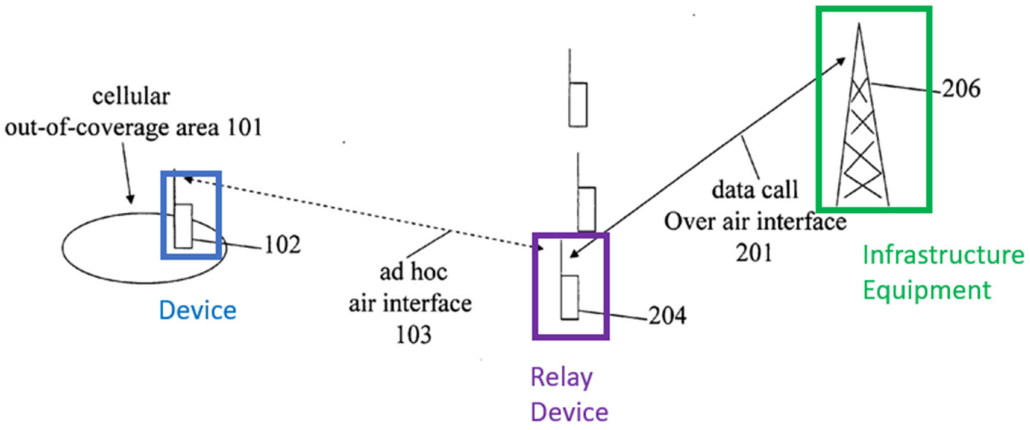
##### (a) Pregont

Pregont addresses situations where a device in one area cannot communicate directly with infrastructure equipment. SAMSUNG-1012, [0003].




SAMSUNG-1012, FIG. 1 (annotated)

In response, Pregont describes relaying calls using ad-hoc networking where a device communicates with a relay device via ad-hoc air interface, and the relay device relays the communication to infrastructure via air interface. SAMSUNG-1012, [0003], [0011].




SAMSUNG-1012, FIG. 2 (annotated)

Per Pregont, to relay a call, the relay device must "hold a simultaneous call over the ad hoc link ... and the cellular link." *Id.*, [0004]. The communication unit includes cellular and ad-hoc receivers and transmitters. SAMSUNG-

1012, [0020].

In Pregont, when the relay device receives a request from the device, the relay device starts a data call (e.g., VoIP) over the cellular link using the relay device's data capability. SAMSUNG-1012, Abstract.

Pregont explains that the relay device must simultaneously make its own calls, so during a relayed call, the relay device uses the existing data call to piggyback a message to the infrastructure equipment, and "the two VoIP sessions would co-exist on the single data session between the cellular phone and the infrastructure equipment." SAMSUNG-1012, [0004], [0012].

(b) **Combination**

Rao describes a computing device with applications, e.g., IP telephony and other applications. SAMSUNG-1005, [0088], [0179]. Pregont similarly describes a communication device, capable of making calls and relaying traffic simultaneously. SAMSUNG-1012, [0004], [0011]-[0012]. To enable Rao's device to extend the communication range of other devices, a POSITA would have been motivated to include Pregont's call-relay application as an additional application on Rao's device. SAMSUNG-1003, ¶[214]. The resulting device both executes applications, per Rao, and relays telephony traffic, per Pregont. SAMSUNG-1005, [0179]; SAMSUNG-1012, [0011]-[0012]; SAMSUNG-1003, ¶¶[214]-[216].

A POSITA would have understood that, when multiple applications use the network, network bandwidth can be exhausted. SAMSUNG-1003,

¶[215](citing SAMSUNG-1054). In such cases, to avoid overwhelming network capacity, adversely impacting all device applications, a POSITA would have looked to references such as Jones, which teaches that applications can be denied network access when bandwidth is insufficient. SAMSUNG-1006, 5:13-15; SAMSUNG-1003, ¶[217].

As described above, Pregont uses VoIP to communicate between the relay device and the communication infrastructure. SAMSUNG-1012, Abstract. As discussed above, Jones teaches applying rules "to data transfers depending on the ... connection bandwidth" and such rules "may prohibit data transfers." SAMSUNG-1006, 5:13-26; §III.K.1.b. Thus, a POSITA would have recognized that, when RD's bandwidth is constrained, it would advantageously benefit from prohibiting data transfers, per Jones, e.g., by the relay application (a type of functionality, as described in Jones). SAMSUNG-1003, ¶[218].

The resulting Rao-Pregont-Jones Device (RPJD) is a mobile device (per Rao) that provides relay services to other devices (per Pregont). SAMSUNG-1005, [0086]-[0096]; SAMSUNG-1012, [0004], [0011]-[0012]. When a different communication device is outside cell coverage, it connects to RPJD, which provides relay services (using VoIP) between that device and the infrastructure equipment, per Pregont. SAMSUNG-1012, [0004], [0011]-[0012]. Additionally, per Jones, RPJD determines whether sufficient bandwidth exists for the relay application; if not, RPJD denies network access to the relay application. SAMSUNG-1006, 5:13-26; SAMSUNG-1003, ¶¶[218]-[219]. Per Jones, RPJD

presents "a graphical user interface," enabling policies to be "configured by a user such as a system administrator." SAMSUNG-1006, 6:36-41; SAMSUNG-1003, ¶[220].

RPJD includes a GUI enabling policies to be "configured by a user such as a system administrator." SAMSUNG-1006, 6:36-41.

The components of RPJD each operate similarly to how they operate in isolation. SAMSUNG-1003, ¶[221]. A POSITA would have a reasonable expectation of success in creating the combination. *Id.* Indeed, the change would have amounted to nothing more than the use of a known technique to improve similar mobile devices in a similar way and combining prior art elements according to known methods to yield the predictable results described above. *Id.*; *KSR*, 550 U.S. at 417.

**2. Analysis**

***[1.1]-[1.7a]***

RPJD renders [1.1]-[1.7a] obvious. *See* §III.A.2.[1.1]-[1.7a].

***[1.7b]***

RPJD renders [1.7b] obvious. SAMSUNG-1003, ¶¶[391]-[393].

Jones teaches that rules include a condition aspect that can depend on functionality and connection bandwidth. SAMSUNG-1006, 5:13-15. The condition aspect assists in determining whether to apply the action aspect, which "may prohibit data transfers." SAMSUNG-1006, 5:25-26; SAMSUNG-1003, ¶[392]. Thus, a POSITA would have recognized that the condition aspect of

RPJD's control policy assists in preventing access by the first application (Pregont's telephony relay). SAMSUNG-1003, ¶[392]; §III.K.1.b.

***[1.7c]***

RPJD teaches or renders [1.7c] obvious. SAMSUNG-1003, ¶¶[394]-[396].

The condition aspects in Jones's policies can depend on functionality and connection bandwidth. SAMSUNG-1006, 5:13-15. Pregont's telephony relay application uses the cellular link for a data call (VoIP call). SAMSUNG-1012, Abstract. Other RPJD applications (e.g., video conferencing) provide different functionality and use different connection types, so conditions that evaluate to TRUE for Pregont's telephony relay application will evaluate to FALSE for other RPJD applications. SAMSUNG-1003, ¶[395]. Thus, a first control (blocking network access) applied to the first application (telephony relay) will differ from a second control (allowing access) by a second application (e.g., video conferencing). SAMSUNG-1003, ¶[396]; §III.K.1.b.

***[1.8]***

RPJD renders [1.8] obvious.

Jones teaches that applying the policy "may prohibit data transfers," which a POSITA would have recognized as preventing access. SAMSUNG-1006, 5:25-26; SAMSUNG-1003, ¶[398].

***[24]***

RPJD renders [24] obvious. SAMSUNG-1003, ¶¶[399]-[402].

RPJD's telephony relay provides a forwarding service between a device coupled to RPJD and a network system. SAMSUNG-1003, ¶[400]. In Pregont, when the device receives a request to relay a call, it starts a data call (VoIP) over the device's cellular link. SAMSUNG-1012, Abstract.

Further, the condition aspect of RPJD's control policy assists in determining whether the telephony forwarding service is available to a second communication unit. SAMSUNG-1003, ¶[401]. For example, Jones teaches that policies can depend on "connection bandwidth," so if sufficient connection bandwidth is unavailable, RPJD prohibits data transfer from the telephony relay application, thereby making the forwarding service unavailable to other devices. SAMSUNG-1006, 5:13-26; SAMSUNG-1003, ¶[402]; §III.K.1.b.

## IV. §314(a) DISCRETION SHOULD NOT PRECLUDE INSTITUTION

The merits of Petitioner's arguments are compelling, and the evidence in support is substantial. That "alone demonstrates that the PTAB should not discretionarily deny institution under *Fintiv*." SAMSUNG-1020, 4-5. Moreover, the *Fintiv* factors do not favor denial.

***Factor 1*** is neutral; neither party has requested a stay in co-pending litigation.

***Factor 2*** is neutral because the Court's trial date (October 2025) is subject to change. The Board will likely issue its Final Written Decision late December 2025. The median time-to-trial time is 21.4 months, projecting a

mid-October 2025 trial. SAMSUNG-1017, 35. However, "scheduled trial dates are unreliable and often change." SAMSUNG-1015, 8.

***Factor 3*** favors institution; Petitioner has filed this Petition months ahead of the one-year time bar, while the EDTX Litigation is still in its early stages. Beyond exchanging preliminary infringement/invalidity contentions, the parties have yet to expend significant resources on invalidity.

***Factor 4*** favors institution because Petitioner has provided a stipulation that it will not pursue the IPR grounds in the EDTX Litigation. SAMSUNG-1016. Thus, "[i]nstituting trial here serves overall system efficiency and integrity goals by not duplicating efforts and by resolving materially different patentability issues." *Apple, Inc. v. SEVEN Networks, LLC*, IPR2020-00156, Paper 10, 19 (June 15, 2020); *see Sand Revolution II, LLC v. Continental Intermodal Group-Trucking LLC*, IPR2019-01393, Paper 24, 12 (June 16, 2020).

***Factor 5:*** The parties in the parallel litigation are the same.

***Factor 6*** favors institution; the merits of this Petition are compelling.

## V. CONCLUSION AND FEES

The Challenged Claims are unpatentable. Petitioner authorizes charge of fees to Deposit Account 06-1050.

## VI. MANDATORY NOTICES UNDER 37 C.F.R § 42.8(a)(1)

### A. Real Party-In-Interest Under 37 C.F.R. § 42.8(b)(1)

Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, "Samsung") are the real parties-in-interest.

### B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

The '811 Patent is the subject of civil action *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al.*, 2-23-cv-00641 (EDTX), filed December 29, 2023 (SAMSUNG-1004). Petitioner is not aware of any other disclaimers, reexamination certificates, or IPR petitions addressing the '811 Patent.

### C. Lead And Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Petitioner provides the following designation of counsel.

| Lead Counsel | Backup counsel |
|---|---|
| W. Karl Renner, Reg. No. 41,265<br>Fish & Richardson P.C.<br>60 South Sixth Street, Suite 3200<br>Minneapolis, MN 55402<br>Tel: 202-783-5070<br>Fax: 877-769-7945<br>Email:IPR39843-0180IP1@fr.com | Jeremy J. Monaldo, Reg. No. 58,680<br>Jennifer J. Huang, Reg. No. 64,297<br>60 South Sixth Street, Suite 3200<br>Minneapolis, MN 55402<br>Tel: 202-783-5070<br>Fax: 877-769-7945<br>PTABInbound@fr.com |

### D. Service Information

Please address all correspondence and service to the address listed above. Petitioner consents to electronic service by email at IPR39843-0180IP1@fr.com (referencing No. 39843-0180IP1 and cc'ing PTABInbound@fr.com, axf-ptab@fr.com, jjm@fr.com and jjh@fr.com).

Respectfully submitted,

Dated June 18, 2024

/Jennifer J. Huang/

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Jennifer J. Huang, Reg. No. 64,297
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. IPR2024-01051)

Attorneys for Petitioner

**CERTIFICATION UNDER 37 CFR § 42.24**

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 13,826 words, which is less than the 14,000 allowed under 37 CFR § 42.24.

Dated June 18, 2024

/Jennifer J. Huang/

W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Jennifer J. Huang, Reg. No. 64,297
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Attorneys for Petitioner

**CERTIFICATE OF SERVICE**

Pursuant to 37 CFR §§ 42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on June 18, 2024, a complete and entire copy of this Petition for *Inter Partes* Review and all supporting exhibits were provided by Federal Express, to the Patent Owner, by serving the correspondence address of record as follows:

Headwater Research LLC
C/O Farjami & Farjami LLP
26522 La Alameda Ave., Suite 360
Mission Viejo, CA 92691

/Diana Bradley/
Diana Bradley
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(858) 678-5667